NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DESIGN AND ANALYSIS OF A MODEL RECONFIGURABLE CYBER-EXERCISE LABORATORY (RCEL) FOR INFORMATION ASSURANCE EDUCATION

by

R. James Guild

March 2004

Thesis Advisor:	Cynthia E. Irvine
Co-Advisor:	J.D. Fulp

Approved for public release; distribution is unlimited.

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Design and Analysis of a Model Reconfigurable Cyber-Exercise Laboratory (RCEL) for Information Assurance Education			**5. FUNDING NUMBERS**
6. AUTHOR(S) Mr. R. James Guild			
7. PERFORMING AGENCY NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING AGENCY REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES This material is based upon work supported by the National Science Foundation under Grant No. DUE-0210762. NSF support also must be orally acknowledged during all news media interviews, including popular media such as radio, television and news magazines. Except for articles or papers published in scientific, technical or professional journals, the following disclaimer must be included: The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited.			**12b. DISTRIBUTION CODE**
13. ABSTRACT ***(maximum 200 words)*** This thesis addresses the need to create a flexible laboratory environment for teaching network security. For educators to fully realize the benefit of such a facility proto-type exercise scenarios are also needed. The paper is based on a model laboratory created at the Naval Postgraduate School. The initial configuration of the NPS lab is described. The work then develops a list of learning objectives achievable in the RCEL. Six proto-type cyber-exercise scenarios are presented to supplement the RCEL description. The activities of each potential scenario are described. Learning objectives met during each scenario are shown. This thesis work demonstrates how a variety of potential RCEL exercises can supplement traditional information assurance education delivery techniques.			
14. SUBJECT TERMS Computer Science Education, Information Security, Cyber-Exercise, computer security training, information assurance training, computer laboratory			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited.

DESIGN AND ANALYSIS OF A MODEL RECONFIGURABLE CYBER-EXERCISE LABORATORY (RCEL) FOR INFORMATION ASSURANCE EDUCATION

R. James Guild
Civilian, Federal Cyber Service Corps, Naval Postgraduate School
B.S. California Lutheran University, 1986
MMIS West Coast University, 1988

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN COMPUTER SCIENCE

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: R. James Guild

Approved by: Dr. Cynthia E. Irvine
Thesis Co-Advisor

J.D. Fulp
Thesis Co-Advisor

Dr. Peter Denning
Chairman, Department of Computer Science

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

This thesis addresses the need to create a flexible laboratory environment for teaching network security. For educators to fully realize the benefit of such a facility, proto-type exercise scenarios are also needed. The paper is based on a model laboratory created at the Naval Postgraduate School. The initial configuration of the NPS lab is described. The work then develops a list of learning objectives achievable in the RCEL. Six proto-type cyber-exercise scenarios are presented to supplement the RCEL description. The activities within each potential scenario are described. The learning objectives met during each scenario are shown. This work demonstrates how a variety of potential RCEL exercises can supplement traditional information assurance education delivery techniques.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

The preparation of this thesis was aided by the help and guidance of Mr. Scott Coté, Capt. Francis Afinidad, and Mr. Paul Pappas of Gambit Communications aided the preparation of this thesis. I especially wish to thank my loving wife Jennifer, who joined me as a student in this adventure at NPS, for her love and patient support. I would also like to acknowledge my thesis advisors Mr. Fulp and Dr. Irvine.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PURPOSE OF STUDY

The intent of this thesis is twofold; first, to demonstrate how a Reconfigurable Cyber Exercise Laboratory (RCEL) can be designed and used in support of an information assurance education program. Second, to design six cyber exercise scenarios that can be used as models for other information assurance programs.

Within this thesis, the author will describe the RCEL implemented at NPS, the stations and the services implemented in that facility. Next, the paper will develop learning objectives achieved through activities in the RCEL. The learning objectives will then be related to courses in an information assurance program. The information assurance curriculum of the Naval Postgraduate School will be used as a foundation for this analysis.

With the educational foundation in place, six practical cyber exercise scenarios will be described. Each exercise scenario presents a different use for the RCEL and associates the exercise with learning objectives, classes and supporting documents referenced in this work.

B. SCOPE OF THIS WORK

1. Research Questions

The research questions to be addressed by this thesis will focus on solving the complex issues related to establishing a supportive, realistic laboratory environment in which information assurance topics can be safely explored. When building a RCEL to provide enhanced teaching and learning opportunities within an information assurance curriculum, the following questions must be addressed:

1. What interaction opportunities exist between a RCEL and concurrently presented information assurance courses?
2. What equipment is needed (minimum and optimal) in this facility?
3. What services or stations should be available in the RCEL?

4. What are the optimal security procedures and policies for each service, OS, and device in the RCEL?
5. How can a RCEL organization achieve safe interaction with external RCELs in both attack and defense postures?
6. What security concepts and practices can be effectively presented in the RCEL?
7. What exercise scenarios demonstrate effective use of the RCEL?

2. Research Objectives

This thesis will present the following:

1. To identify existing academic standards, (if any), directly related to computer security education.
2. To propose a flexible topology that models a general-purpose network that is rapidly reconfigurable and supports the study of IA topics.
3. The thesis will develop a list of learning objectives and their mapping to the prototype exercise scenarios.
4. To define six proto-type cyber-exercise scenarios that provide effective models for security exercises.
5. The thesis will present relevant information needed to conduct post-exercise analysis of the exercise data.

II. THE NAVAL POSTGRADUATE SCHOOL RECONFIGURABLE CYBER-EXERCISE LABORATORY

A. JUSTIFICATION FOR THE CREATION OF A RECONFIGURABLE CYBER-EXERCISE LABORATORY TO SUPPLEMENT TRADITIONAL INSTRUCTION

Tables 1 and 2 are from the SANS (SysAdmin, Audit, Network, Security) Institute web site (http://www.sans.org/resources/errors.php#top). Table 1 emphasizes the need for good information assurance (IA) and cyber-security education. Note, that of the seven management errors listed, all can be mitigated through information assurance education.

Table 1. The 7 Top Management Errors that Lead to Computer Security Vulnerabilities (As determined by the 1,850 computer security experts and managers meeting at the SANS99 and Federal Computer Security Conferences held in Baltimore May 7-14, 1999)

Number Seven:	Pretend the problem will go away if they ignore it.
Number Six:	Authorize reactive, short-term fixes so problems re-emerge rapidly
Number Five:	Fail to realize how much money their information and organizational reputations are worth.
Number Four:	Rely primarily on a firewall.
Number Three:	Fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed
Number Two:	Fail to understand the relationship of information security to the business problem -- they understand physical security but do not see the consequences of poor information security.
Number One:	Assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job.

Before expounding on the specific learning objectives addressable in the reconfigurable cyber-exercise laboratory (RCEL), it is essential to understand what kind of issues IA practitioners should be aware of. Again, referring to research conducted at the SANS Institute, we see in Table 2 that the most egregious security problems are spawned by the IT staff.

Table 2. Top 10 Mistakes IT Professionals Make Regarding Security

Number 1	Connecting systems to the Internet before hardening them.
Number 2	Connecting test systems to the Internet with default accounts/passwords
Number 3	Failing to update systems when security holes are found.
Number 4	Using telnet and other unencrypted protocols for managing systems, routers, firewalls, and PKI.
Number 5	Giving users passwords over the phone or changing user passwords in response to telephone or personal requests when the requester is not authenticated.
Number 6	Failing to maintain and test backups.
Number 7	Running unnecessary services, especially ftpd, telnetd, finger, rpc, mail, rservices
Number 8	Implementing firewalls with rules that don't stop malicious or dangerous traffic-incoming or outgoing.
Number 9	Failing to implement or update virus detection software
Number 10	Failing to educate users on what to look for and what to do when they see a potential security problem.
Number 11 (Bonus cause)	Allowing untrained, uncertified people to take responsibility for securing important systems.

The reconfigurable cyber-exercise laboratory(RCEL) used in an academic program addresses the issues raised by the SANS Institute and provides an opportunity for students to learn effective IA practices in a safe environment. The RCEL, however, goes far beyond just hands-on training. It empowers the instructor or professor to follow the three critical steps of learning: show, demonstrate, and do [ELE01].

In an ERIC Digest (Educational Resource Information Clearinghouse, now defunct) published in 1997, Travis, stated regarding models for improving college teaching:

> As learning becomes more complex, students frequently depend upon faculty to assist them with a multitude of obstacles. Yet, given the typical preparation college faculty receive for teaching (ed. little or none), the tendency to concentrate on presentational methods, like the lecture, can aggravate students' difficulties with learning. Consequently, instructors are encouraged to stop viewing teaching as “covering the content” and to start viewing it as "helping the students learn" [WEI01]

Teaching and learning information assurance is challenging. Often traditional teaching methods are not adequate or comprehensive. For some students, gaining a

through understanding of IA is not fully achievable in a classroom. A student's learning experience is enhanced when they have configured a router, perpetrated or been the victim of an attack and "experienced" security. The RCEL provides that hands-on experience to supplement traditional presentation. In Figure 1, learners who supplement traditional educational with hands-on activities remember 90% of the lesson compared to only 20% from a traditional lecture [DAL01].

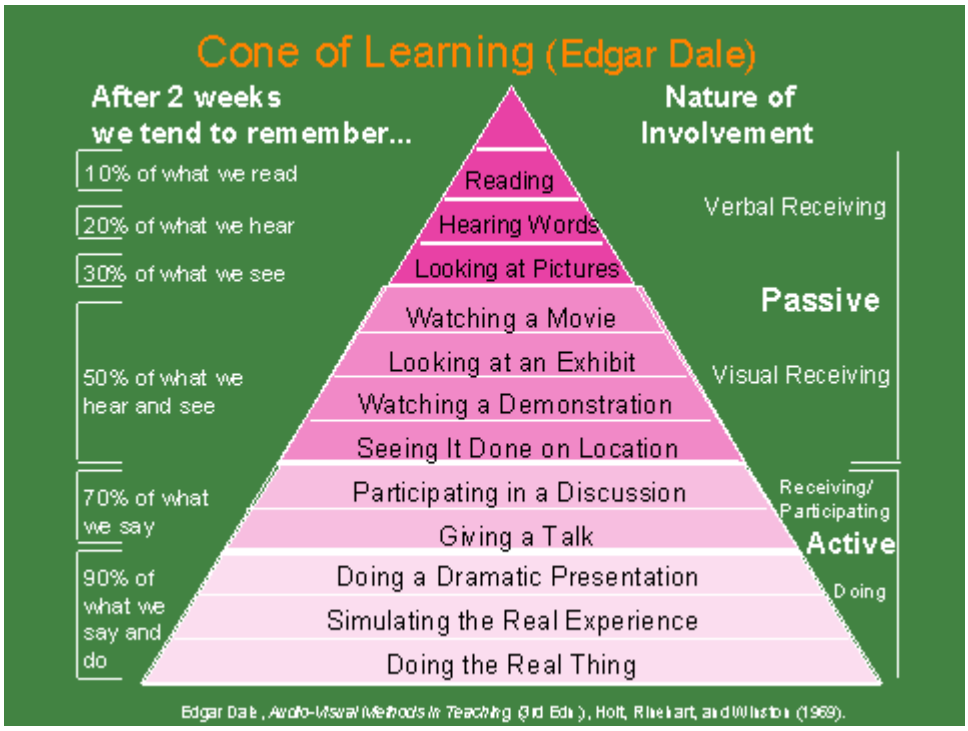

Figure 1. Edgar Dale's Cone of learning [DAL01]

B. NPS RCEL OVERVIEW

A RCEL is a computer laboratory facility which can be rapidly changed to accommodate various activities. Traditional computer laboratories tend to be static in configuration and difficult to change. The RCEL is a flexible collection of equipment that can be quickly interconnected and configured. Organizations can develop configurations for each piece of equipment or functionality. These configurations can be stored and when needed deployed quickly using like Symantec Ghost.

Unlike a traditional computer lab that must support many students performing a wide variety of activities, the RCEL need not have any specific configuration. The type

and scope of activities to be conducted determines the design, layout, and interconnection requirements. The RCEL need only have sufficient equipment to provide a meaningful network environment.

Figure 2 shows a minimal RCEL exercise configuration. Each LAN (Local Area Network) is achievable with as little as a router and a computer. In Figure 2, the VPN (Virtual Private Network) gateway is any VPNcapable device i.e., a router, computer, or dedicated appliance. The LAN on either side can be any combination of network-attachable devices. The size and complexity of the LAN is based on the needs and resources of the organization. The attacker and defender LANs need not have matching configurations.

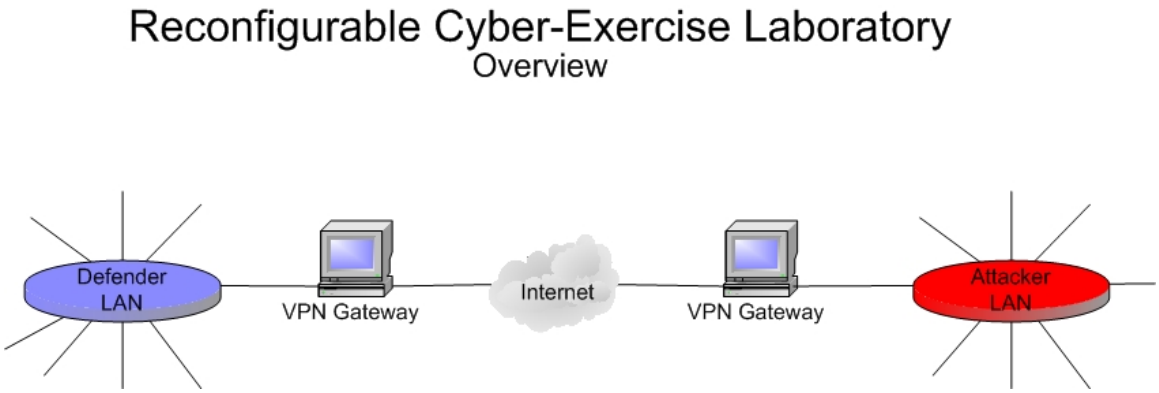

Figure 2. RCEL Concept Diagram

1. Requirement for VPN

A critical design requirement is the isolation of exercise traffic from any public networks. Figure 2 shows the fundamental structure of an attack/defend exercise. VPN Gateways isolate each LAN from the public Internet. Note, the "Internet" cloud is any ISO layer 1 and 2 configuration for passing IP traffic. The only functional requirement on this "internet" is that it must provide functional connectivity between the VPN gateways. The secure configuration of the VPN Gateways is critical when the RCEL is connected to another organization via the real Internet. The VPN is discussed in detail in Chapter VI.

If the attacker and defender are within the same organization and their respective networks are air-gapped from any other network, the VPN is unnecessary. However, the RCEL described in this work assumes the attacker and defender are sufficiently remote to necessitate internetworking across some portions of the public infrastructure.

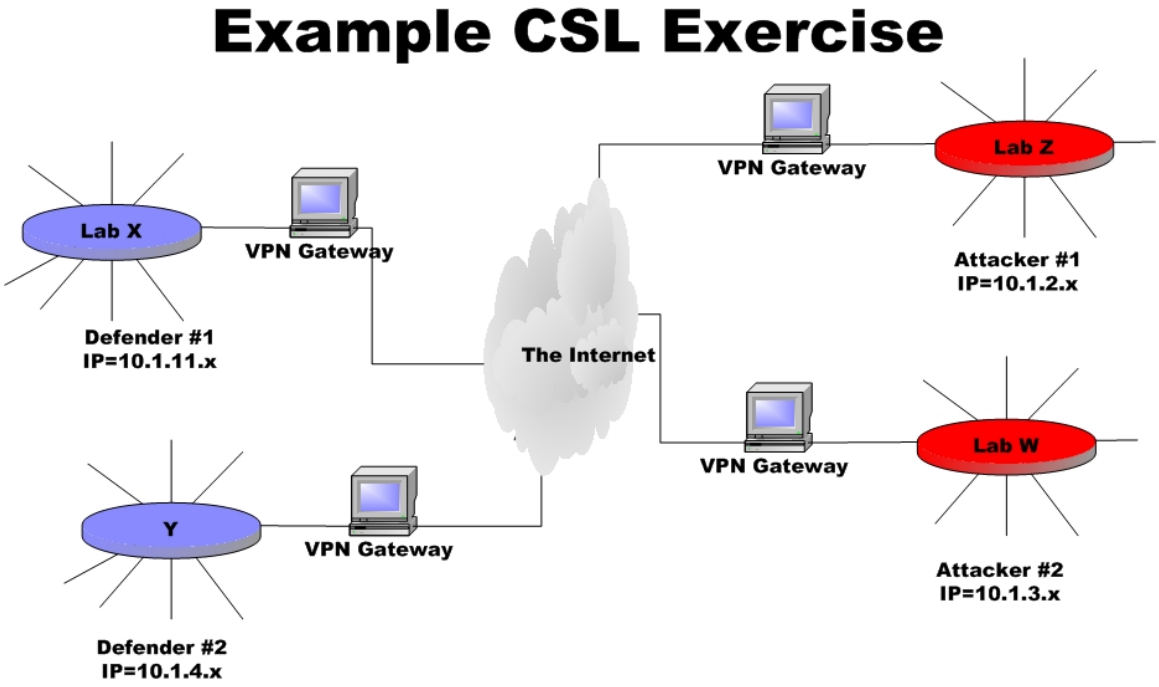

Figure 3. Example Security Training Exercise

Figure 3, shows how four organizations might interact and interconnect for a cyber exercise. When the VPNs are in place and working correctly, there is no danger of spillover onto networks or devices traversed between locations.

The Attacker LAN may use any means (agreed upon by the interacting organizations) to breach the systems of the Defender LAN. This includes any form of malware as well as more interactive exploits. The activity of the Attacker is cryptographically constrained within the VPN tunnel and therefore is allowed to pass across public networks to reach the Defender.

The Defender/Attacker LAN consists of various interconnected computers. The RCEL configured at the Naval Postgraduate School (NPS) was interconnected via Cat-5 [NAT17] cabling in a 10/100 Base-T Ethernet configuration.

An air-gapped lab was chosen for the RCEL, but one in which access to the campus LAN was possible (though carefully controlled). The NPS RCEL maintains at least one computer that is not part of the scenario lab, but is connected to the campus LAN, that is made available for research and communication, mostly e-mail. This dedicated machine has proven very useful in downloading patches and software tools to strengthen the network, as well as documents for help and guidance. (For a more detailed description of this access station, see Station Description 23 below.)

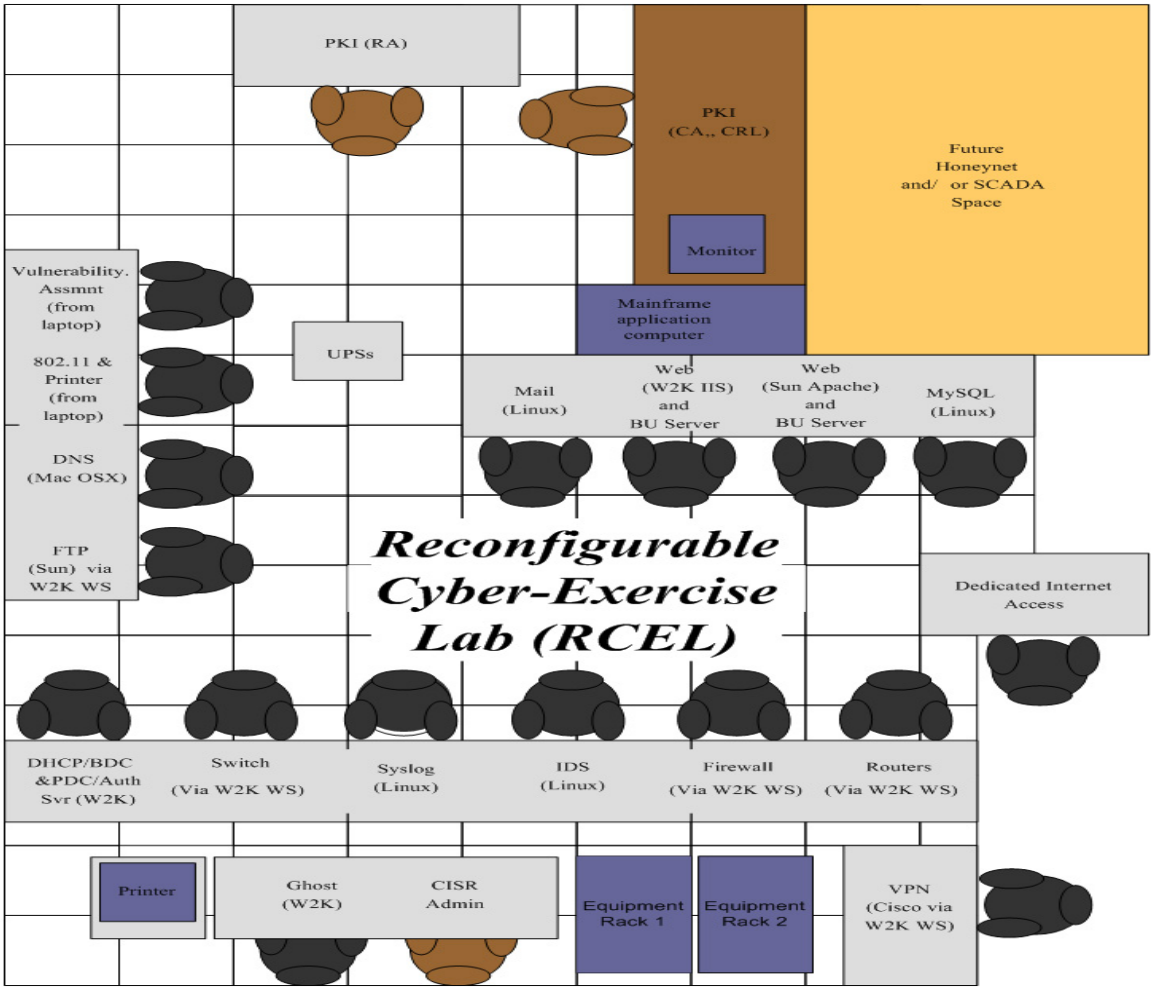

Figure 4. NPS RCEL Stations

Figure 4 shows the physical layout for the Naval Postgraduate School‘s RCEL. The Naval Postgraduate School has set up the RCEL with as few as three people, each assigned to several stations. The design allows 18-24 students to participate comfortably. Each seat represents a specific network function such as IDS or Firewall, which can be

assigned to an individual or team. Each location has a monitor which may be connected to any of several computers or a laptop. Multiplexing of each seat is accomplished using KVM (Keyboard, Video, Mouse) switches which allow a single station to connect with up to four computers.

C. NAVAL POSTGRADUATE SCHOOL RECONFIGURABLE CYBER-EXERCISE LABORATORY NETWORK DESIGN

The NPS RCEL utilized existing equipment, which was in place as a result of previous acquisitions and funded exercises. The equipment currently includes: 16 Dell Servers, 1 Apple G4, Cisco 4224 Layer 3 switch, Cisco Routers (numerous), Cisco PIX 506 Firewall, 2 Dell Laptops, 2 Sun Netra X1 servers, numerous small hubs and switches. The RCEL also benefits from relationships with local corporations For example, Cisco Systems recently donated several routers, switches, and a Pix 506 firewall.

Figure 5[1] presents the general topology of the NPS RCEL network. The topology is based on the concept that the NPS RCEL is the Top Level DNS Domain for this and any attached networks.

In the topology, hubs 1,2 & 3 are treated as non-existent: they have no impact on security. These "non-existent" hubs are part of the data collection package that provides a means for assessment and monitoring. Connections shown with dotted lines are transient; i.e., they indicate connectivity that may be put in place when needed.

[1] The topology was developed by Mr. Ken Johns, Ms. Jennifer Guild and the author.

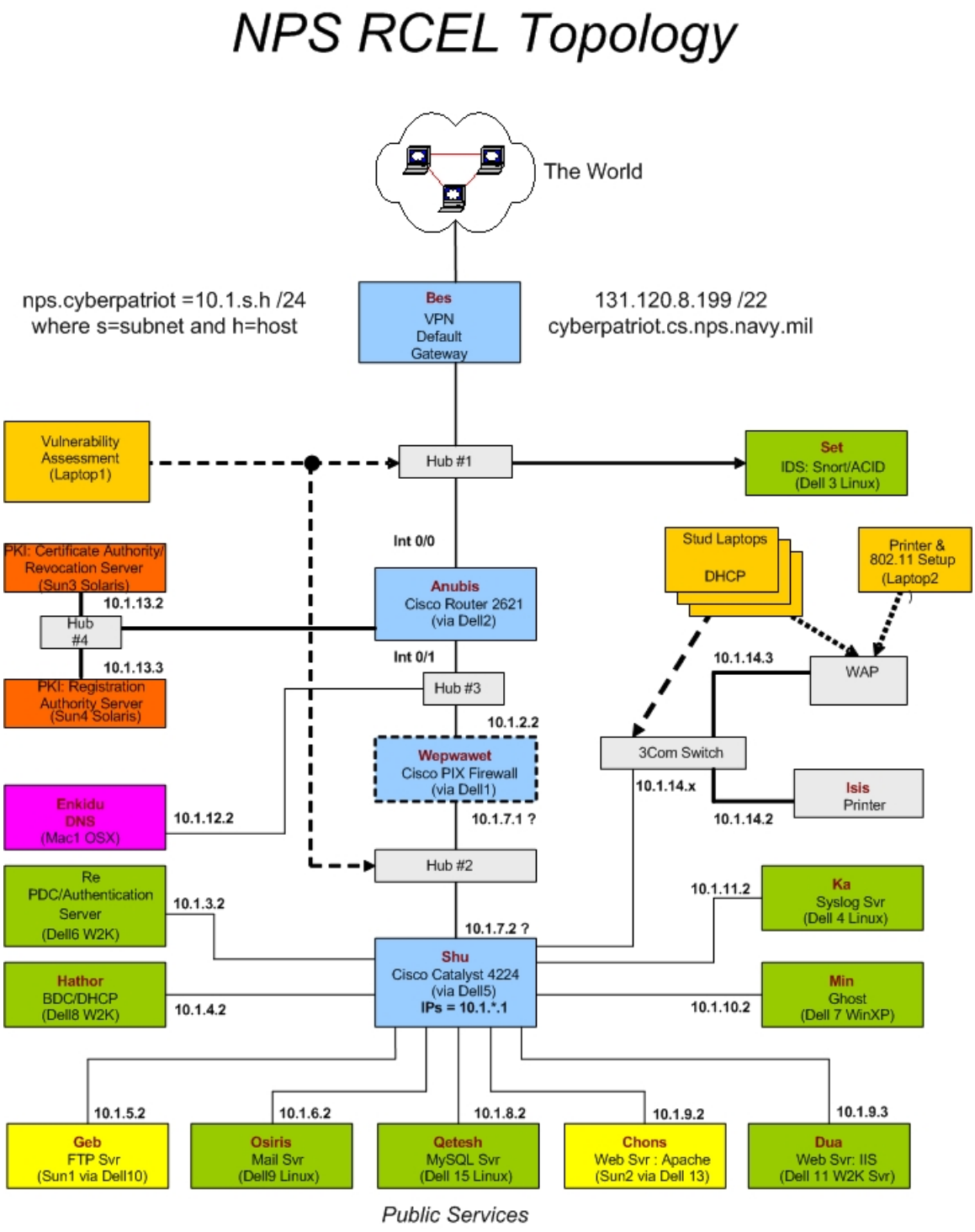

Figure 5. NPS RCEL Topology

To give the student a realistic experience managing complex networks **t**he NPS RCEL uses subnets and makes extensive use of VLANs. In the topology in Figure 5,

server IP addresses are fixed and correspond to the VLAN (Virtual Local Area Network) to which the server is associated. Dynamic Host Configuration Protocol (DHCP)[DRO01] addresses are provided for individual non-server workstations. Employing VLANs provides the opportunity for the students to create ACLs (Access Control Lists) for the Cisco switch and perform specific filtering for each network segment based on that segment's functions and applications.

Designing a RCEL can be taken to extremes. For example, networks can be constructed with VPN (Virtual Private Network) encrypted tunnels between every major device (refer to RFCs 2401, 2406, 2407, 2408 and 2409), complex naming schemes, exhaustively long and complex passwords, encryption on all data moving between devices and so on. Such complexity, while apparently increasing security, is very hard to maintain. In the book *Security in Computing*, Pfleeger [PFL01] argues complexity actually decreases the overall security due to increased likelihood of configuration mistakes, and the added complexity of managing and verifying correct security implementation. An effective RCEL then is a balance of functionality, security and student usability.

The RCEL is designed to incorporate as much functionality of a real network environment as possible. The network operating system (NOS) of the network shown in Figure 5 resides on the PDC and BDC servers. The NOS provides the applications that deliver network services such as authentication and domain control. The NOS for the RCEL at NPS is Microsoft Windows 2000 Server.

D. STATIONS WITHIN THE RECONFIGURABLE CYBER-EXERCISE LABORATORY

For educational purposes, the RCEL is organized into a number of "stations." Each station is defined as an area of responsibility which can be assigned to a student or group. In keeping with Saltzer and Schroeder's design principles of economy of mechanism and separation of privilege [SAL01], each station has a singular purpose , e.g., to provide network authentication or provide network switching. Students assigned to a particular station are expected to "get to know" that station thoroughly and how that station integrates into the larger RCEL network.

The station concept provides flexibility while providing a measure of control and accountability over students. Stations can be assigned by student interest, skill, availability or any scheme suitable to the circumstances of the exercise.

Within the NPS RCEL, 23 stations have been identified and are described below. A * indicates stations that are planned but not implemented and ** indicates a station that is not connected to any of the others as of the completion of this document (March 26, 2004).

1. Authentication – This station establishes and manages the network authentication service. Users are required to authenticate to some network service such as X-500 (An OSI protocol for managing online directories of users and resources.), Active Directory, or Novell. The station manager installs and configures the authentication technique and associated software and hardware to be used.
2. PDC (Primary Domain Controller) - The PDC holds the SAM (System Account Manager) Sam is a password database stored as a registry file in Windows based networks and authenticates access requests from workstations and servers in the domain. The Authentication service may be combined with this station. The person(s) assigned to this station would implement and manage this functionality in accordance with the network architecture plan.
3. BDC (Backup Domain Controller) – As the name implies, this server backs up the PDC in case of failure (or attack). The most important role here is managing how the network switches to the BDC in the event on an interruption of the PDC.
4. Vulnerability Assessment – This station is used to port scan, enumerate and probe the associated network to assess the effectiveness of the implemented security plan. This station is a laptop (in the NPS RCEL) connected only for testing and monitoring purposes. It is not considered part of the active network and is connected to the network at any point to provide active testing or data collection via a dumb hub. The manager of

this station is responsible for acquiring the vulnerability assessment tools, knowing their proper use, performing active probing and vulnerability assessments and reporting results to those responsible for configuring the servers or services.

5. DNS (Domain Name System) – The DNS server provides a query service used for translating hostnames into IP addresses. The functionality of the DNS server is specified by IETF (Internet Engineering Task Force) STD 13 [MOC01]. STD 13 is published by the Internet Engineering Task Force specifies standards and implementation characteristics of DNS. There are numerous publicly available DNS implementations. The Naval Postgraduate School chose DJBDNS (available from http://ww.djbdns.org) for the RCEL[DJB01].
6. FTP (File Transfer Protocol) – This station provides a server running the FTP server daemon. This service allows users to move data into (FTP put) and out (FTP get and mget) of the server. The file transfer protocol is specified in RFC-959 [POS01]. There are many FTP vulnerabilities and exploits. A recent (January 2004) search of the CERT database found 282 (http://www.cert.org) exploits and vulnerabilities related to FTP services.
7. *PKI CA/RA(Public Key Infrastructure Certificate and Registration Authority) [NAT02]– This station will include a local certificate authority which will be able to issue, revoke and validate PKI certificates to users. These certificates are only valid on the RCEL network or other exercise-participant networks attached via the VPN.
8. Email – This station implements an email server such as MS Exchange, Eudora, Linux email server, etc. The choice of software is decided in the analysis and design of the network. Each organization may have a preference or constraint that determines the choice of email service. The NPS RCEL implements Linux mail (because it is free). Email distribution and security rules are in accordance with the particular exercise security

plan. Like FTP, E-mail is another primary source of intrusion by outsiders. The proper security configuration of this service is crucial.

9. Web – This station provides Web services in as specified in RFC-1945 [BER02]. It is one of the most vulnerable parts of the network as the web server must allow access to fulfill its primary function of delivering content. The manager of this station implements web pages that provide the necessary functionality to access databases, run CGI (Common Gateway Interface) scripts and Java scripts. This station is a primary target for attack.

10. *Wireless – Wireless access points allow authorized users with wireless devices to access the RCEL network. The manager of this station must carefully guard against access by non-RCEL users. The manager must also be knowledgeable, or willing to learn, about wireless technology and the implications of implementing wireless solutions. To prevent the "parking lot" attack described by Arbaugh[ARB01] strong authentication is required. Implementing this station involves not only the primary RCEL instructor, but the local network administrator as well.

11. *HoneyNet – The manager of this station will be responsible for implementing the selected HoneyNet product and writing the proper router scripts to direct selected traffic into the trap. Although a lot of legal wrangling is currently making the news regarding HoneyNet [PFL01, MCC01] implementations, this station provides a useful learning tool in the RCEL. In addition to traditional HoneyNet products, unique technologies such "La Brea Tar Pits" software or other "sticky" solutions can be implemented and tested.

12. *SCADA (Supervisory Control and Data Acquisition) – The CISR, Center for Information Systems Security Studies and Research, has acquired the equipment for, and is active in, SCADA research. As that effort matures, SCADA might become another dimension of the RCEL in

the future. Not all schools/agencies that implement a RCEL will necessarily be interested in SCADA network security

13. MySQL (Database server) – This station represents a typical data server for a web page. MySQL was chosen as the database simply because it is free and widely supported on the Internet. The database server in the NPS RCEL is configured with MySQL. This choice was made because MySQL is open source. Any significant database engine such as Oracle or MS-SQL or even MS Access can be used for this purpose. The station manager must know SQL and database design. The database typically provides or accepts data from the Web application but may be directly accessed as well. Most modern networks have some data retrieval or search capability, so this station is significant in providing a "real world" aspect to the RCEL.

14. Routers – The RCEL has several routers which can be connected separately or in an HSRP (Hot Standby Routing Protocol) [LAR01] failover configuration. The routers are a key element of the network's perimeter security. The manager of this station(s) will configure the software (i.e., IOS running-configuration file) and write and verify filtering access control lists (ACLs). Most students have not had IOS (Internetwork Operating System, ®Cisco Systems) experience, so it is essential for the instructor to provide assistance. A vast amount of helpful documentation is available on the Internet and from official government sources like the NSA (National Security Agency) and NIST (National Institute of Standards and Technology).

15. Firewall – Like the routers, the firewall is programmed to implement a major portion of the security plan. The RCEL uses a Cisco Pix® 506 firewall which is programmed in IOS like the router. The station manager must program the Firewall to allow or block traffic as appropriate to the exercise. For organizations building an RCEL, other firewall products are available. Each firewall product will have a different configuration

interface and different strengths and weaknesses. Restrictions on which products can be used may apply for organizations within the DoD as not all such products are manufactured in the US.

16. IDS (Intrusion Detection System) – The NPS RCEL IDS station is connected to the border router via a hub. Tapping the network before filtering allows the IDS to collect more traffic to get a better baseline of traffic patterns and to gather the largest amount of data for analysis. Tapping after the firewall would reduce traffic as the easily filtered or nuisance traffic would have been eliminated. As a scholastic environment, NPS chose to gather the maximum amount of traffic to facilitate analysis. NPS uses Snort™ from Snort.org. Snort™ is popular and widely supported by resources on the Internet. The station manager will be required to install and set up Snort™ to comply with the security and analytical requirements developed for the exercise.

17. DHCP (Dynamic Host Configuration Protocol) – This function can be part of the Primary Domain Controller or may exist separately. The manager of this station configures the DHCP service in accordance with the RCEL exercise topology. The purpose of DHCP is to provide IP addresses to stations which do not have IP addresses already assigned to them.

18. Disk Imaging - This station provides backups of setups or configurations in the event a disk is corrupted. The ghost images are captured from a well defined configuration prior to an exercise. The Naval Postgraduate School uses Symantec's Norton Ghost product which is ideal for this task. There are other products for this purpose such as ImagIt 1.0 which can be downloaded as a trial version but is costly to purchase. The station may also use an existing utility like dd(© 1989-2000 AT&T Corp.). The advantage of dd is that forensic duplicates can be made and data extracted when the exercises are over.

19. VPN (Virtual Private Network) NAT15, NAT10, RUS01, MCC01, KEN01, LAR01, FRA01, NAT17]- This station is the most critical station

in assuring RCEL success and security. Since the VPN isolates the RCEL from the Internet, it must be configured carefully and checked thoroughly. The VPN manager will also interact with any other organizations engaged in an exercise, providing critical IP address information and VPN configuration data to allow for successful interconnection between exercise participants.

20. Syslog (Auditing) – [ROS01, DAY01, KEL01, GER01] This station collects error messages and event log information for later analysis. The manager of this station configures not only the syslog server but all reporting servers. The reporting servers are configured to provide specific information in the syslog format [ROS01, DAY01]. Auditing is reviewing and analyzing in some way, electronic or manual, the information captured and stored. [KEL01]. Gerhards [GER01] provides a specific format for arriving syslog information and it is suggested in this work that managers of the syslog station adopt Gerhards' proposed standard.

21. Switches – The switch acts upon the content of the Ethernet frame it receives and forwards the frame to the appropriate outbound Ethernet port. The switch provides isolation between ports and VLANs to allow for traffic segregation and management. The NPS RCEL currently uses a Cisco 4224 Catalyst switch programmed in Cisco IOS v12.0. This switch provides for VLANs with separate ACLs. The exercise activities for any given configuration will be the guide for setting up the switch. NSA and NIST provide some excellent guides [NAT16, NAT17], and suggested configurations for network switches that serve well as a starting point for switch configuration. Cisco also provides excellent documentation.

22. Printer – Typical configuration of a printer takes only a few minutes. The importance of the printer; however, is not so much in its explicit functionality as in its proper (secure) configuration to prevent hackers from accessing the printer and possibly gaining access to other systems on the RCEL network. Many modern network printers run small web servlets

which are exploitable if visible to the network. These printers also often have open telnet and FTP ports and services. Printers also have a language of their own which can be exploited. For example, Hewlett Packard printers use PCL (Printer Control Language) and PJL (Printer Job Language) to manage and control printing tasks. The PJL code below written and published by a hacker known as LittleW01f [LIT01] will cause a complete denial of service by putting the printer to sleep.

```
#!/bin/sh
NC=/usr/bin/nc
TRUE=/usr/bin/true
ECHO=/usr/bin/echo
while ($TRUE); do
$NC $1 9100X@PJL OPMSG DISPLAY=\"Printer Fault \"
sleep 2
done
```

The manager of the printer station, therefore, has a challenging assignment because few people have experience with printer interfaces and technologies. The learning curve on this station is especially steep.

23. **DIA (Dedicated Internet Access) – This station is added as a convenience to facilitate communication and research on the Internet while the RCEL remains isolated. It is not assigned to a specific student manager, rather the instructor or area manager must ensure this station remains isolated from the RCEL LAN. The DIA station is wired separately and has only one NIC (Network Interface Card) so it cannot be on both networks simultaneously.

Each station also represents some hardware and interconnection into the network (except the dedicated internet access station). When fully implemented, the RCEL will require a lot of time to configure correctly. If only the assigned lab hours of a typical course (usually 2) are used, it will take most of the semester/quarter to achieve optimal full implementation and testing. .

III. SURVEY OF INFORMATION ASSURANCE TOPICS IN THE NAVAL POSTGRADUATE SCHOOL IA CURRICULUM

NPS is one of few schools in the country to have an information assurance track at the Master's level. CISR (The Center for Information Systems Security Studies and Research) oversees the IA track. The curriculum matrix below shows the courses required in the CISR IA track at the Naval Postgraduate School, and is specific to the Scholarship For Service program[SFS01]. The courses in grey are those that specifically address information security topics.

Table 3. Naval Postgraduate School Information Security Course Matrix for SFS Students

1st Quarter (Fall/Spring)	CS 3902 (4-2) Programming Paradigms	CS 3502 (4-2) Computer Comms and Networks	CS 3650 (6-0) Algorithms and Automata	CS 3600 (4-2) Information Assurance: Introduction to Computer Security	CS 4900 (0-2) Technology, Innovation and Leadership I
2nd Quarter (Winter/Summer)	CS 3310 (4-0) Artificial Intelligence	CS 3690 (4-2) Network Security	CS 3204 (3-2) Human-Computer Interaction	CS 3675 (3-2) Network Vulnerability Assessment	CS 4901 (0-2) Technology, Innovation and Leadership II
3rd Quarter (Spring/Fall)	CS 3670 (3-2) Information Assurance: Management of Security Systems	CS 3320 (3-1) Database Systems	CS 4600 (3-2) Secure Systems	CS 4677 (3-2) Computer Forensics	
4th Quarter (Summer/Winter)	CS 0810 Thesis	SW 3460 (3-1) Software Methodology	MV 3202 (3-2) Computer Graphics Programming	CS 4605 (3-1) Security Policies, Models and Formal Methods	
5th Quarter (Fall/Spring)	CS 0810 Thesis	CS 4603 (3-1) Database Security	Track Elective	CS 4680 (3-0) Intro to C&A and CS 4685 (0-2) Case Studies	
6th Quarter (Winter/Summer)	CS 0810 Thesis	CS 0810 Thesis	OS 3307 (4-1) Modeling Practices for Computing	CS 4614 (3-1) Advanced Topics in Computer Security	

In the above matrix, the shaded courses might benefit from practical exercises within the RCEL. The intention of this work is to show representative applications of the RCEL in the context of these and other courses selected from the IA track.

In this chapter, a list of IA topics is presented. There are other possible IA topics covered at other teaching organizations, but this list is reasonably comprehensive, and provides a grounding for any IA program.

Four major concerns of IA are [IRV04]; confidentiality, integrity, availability, and authenticity. Non-repudiation is sometimes included as a fifth major attribute of IA; however, here non-repudiation is considered to be derived from a combination of mechanisms used to achieve integrity and authenticity, and is therefore not treated as a unique attribute. The following definitions are from the NSTISSI No. 4009 National Information Assurance Glossary created by the NSA [CNS01].

> Confidentiality: Assurance that information is not disclosed to unauthorized individuals, processes, or devices. The process of teaching how to enforce confidentiality, therefore, must include an emphasis on cryptography as well as mechanisms for protected communication, access control mechanisms and privacy controls.
>
> Integrity: Quality of an IS [information system] reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security context, integrity is interpreted more narrowly to mean assured detection of accidental or intentional modification of information.

Integrity can only be assured if there is a certainty that data (the resource) was not inappropriately altered. To teach integrity, topics relating to interception, replay, data insertion, data modification, message authentication, hashing, change detection, digital signatures and key management must be included. The following definitions are also from the NSTISSI No. 4009.

> Availability: Timely, reliable access to data and information services for authorized users. Topics related to availability that must be taught in an effective security program include backup strategies, data and system redundancy, interception, blocking, denial of service issues and physical protection.

Authentication: Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. Topics related to authenticity that must be taught separately include the threat related to spoofing data or users, user authentication, shared secrets, digital certificates and digital signatures. There will be overlap with topics relating to the achievement of integrity; however, especially in the area of hashing and digital signatures.

These four critical concerns form the foundation of IA and surface frequently in the NPS IA curriculum. Here they will be used to form the starting point of our identification of topics that can be taught, demonstrated, or discovered in the RCEL. Not all IA topics lend themselves well to RCEL lab exercises. Our focus in this work is on those topics supported by RCEL activities.

A. MODEL IA COURSES AND POSSIBLE RCEL APPLICATION

The Naval Postgraduate School's Computer Science Department's security curriculum (at the time of this writing) contains the courses that will be discussed here. This list is not exhaustive, but rather representative. The list presented gives a broad perspective of the possible uses of the RCEL.

Please note, the following course descriptions are taken from the NPS online catalog (http://cisr.nps.navy.mil/academics.html) and are italicized to distinguish them from the remainder of this work.

1. CS-3600 (4, 2) Information Assurance: Introduction to Computer Security

Provides a comprehensive overview of the terminology, concepts, issues, policies, and technologies associated with the field of Information Assurance. It covers the notions of threats, vulnerabilities, risks and safeguards as they pertain to the desired information security properties of confidentiality, integrity, authenticity and availability for all information that is processed, stored, or transmitted in information systems.

RCEL activities available for the lab section of this class include: examining the exercise network configuration, demonstrating possible vulnerabilities through scanning or probing the network, demonstrating trusted paths by showing login procedures and how the trusted path is called, firewall and router setup can be shown by the attempting to transmit an improper or filtered packet into the network, etc.

There are also many potential applications of cryptography in the RCEL. When the PKI station is activated, it will become even more so (e.g., dynamically issuing server certificates, validating certificates for relying parties, etc.). Existing cryptographic applications include most authentication schemes, the construction and operation of VPN's, and multiple file encryption schemes available on the various operating systems.

2. CS-3670 (3, 2) Information Assurance: Secure Management of Systems

Provides students with a security manager's view of the diverse management concerns associated with administering and operating an automated information system facility with minimized risk. Students will examine both the technical and non-technical security issues associated with managing a computer facility, with emphasis on DoD systems and policies. Students will earn CNSS (formerly NSTISSI) certification for: INFOSEC professional, Systems Administrator, and ISSO.

The point of this class is to teach how to securely manage computer systems. The RCEL provides an excellent example system as opportunities for demonstrating best practices in secure management abound. The great advantage of the RCEL is that a failure of a security practice here is not catastrophic: students can make mistakes in a safe environment.

Activities in the RCEL for this class might include security surveys and checklists, management policy development, implementation and compliance, security properties of the network and how they are implemented, and hands-on writing of ACLs for routers and firewalls. Other activities are limited only by time and the imagination of the instructor.

3. CS-3675 (3, 2) Network Vulnerability Assessment

This course is designed to give the student exposure to Internet security threats in a lab environment. Lectures and labs provide the student with a "hands on" experience with current network attacks and vulnerabilities. Foot-printing, scanning, enumeration and escalation are addressed from an attack prospective. Emphasis on detection and protection of critical data and nodes is addressed. A final project that demonstrates skills and knowledge is required.

During this course, the students are taught how a variety of exploits work and are introduced to tools for scanning, enumerating, and penetrating systems. Use of the RCEL allows students to safely use these tools against a "real" system. In addition, assessing the vulnerability of the RCEL during a student attack exercise and adjusting security in an effort to thwart such activity gives students within the RCEL practical, real experience.

4. CS-3690 (4, 2) Network Security

Addresses the concepts and technologies used to achieve confidentiality, integrity, authenticity and availability in a networked/internetworked environment. Topics include: fundamentals of TCP/IP, switching and routing, core network security principles, firewall types and methodology, packet-level traffic analysis, cryptographic protocols, virtual private networks, and public key infrastructures.

This class starts by strengthening the student's understanding of networking. The RCEL will be a major part of that by allowing the students to actually see and test various aspects of a functioning network.

5. CS-4600 (3, 2) Secure Computer Systems

This course covers implementation of protection for monolithic and distributed secure computer systems. The problems of subversion and confinement are addressed through lifecycle assurance methodologies for highly secure components. Topics include: protection hardware, implementing virtual machines through effective memory management techniques, synchronization mechanisms, critical sections, SWE methodologies, and configuration mgt techniques.

The RCEL can provide a test bed for the Flaw Hypothesis Methodology (FHM) used in this class. For example, red team (attack activities) used in the RCEL during an exercise may serve as empirical proof of the existence of a flaw.

6. CS-4603 (3, 1) Database Security

Course topics include: policies for information integrity and confidentiality of database (DB) systems, modeling of secure DB systems, implementation issues (e.g., atomicity, serialization, and view-based control), security in statistical DBs, security approaches for object-oriented DBs, multi-tier architecture security issues, privacy, aggregation and inference, and military applications of secure DBs.

The RCEL provides for a database station. This station serves as a demonstration platform for database-dependent applications. Many applications, rely on databases to collect, organize and provide data on demand. The students assigned to this station will benefit from the interaction of the database with other stations of the RCEL.

7. CS-4614 (3, 1) Advanced Topics in Computer Security

This course covers advanced topics in software, communications, and data security. Military and commercial INFOSEC policies are studied, including: software and hardware subversions; advances in operating systems, databases and network security; evaluation criteria for secure systems; logics; cryptographic protocols; techniques for implementing supporting policies; and emerging issues.

The RCEL could serve as a demonstration platform for many of the topics discussed in this course.

8. CS-4677 (3, 2) Computer Forensics

Covers the fundamentals of computer forensics in the context of DoN/DoD information operations. Students examine how information is stored and how it may be deliberately hidden and/or subverted. Coverage includes: practical forensic examination and analysis, techniques of evidence recovery, legal preparation of evidence, common forensic tools, the principle of original integrity, disk examination, and logging.

Course exercises may be tailored to examine current and past attacks against the RCEL. It may also be configured to determine how an internal hacker (in the form of the instructor or another class) might compromise the systems. Additionally, a wealth of valuable forensic information will be generated every time an exercise of any scope is conducted.

9. CS-4680 & 4685 (3, 0) (0, 2) Introduction to Certification and Accreditation and System Certification Case Studies

This course provides an introduction to the Certification and Accreditation (C&A) process as applied to procurement and lifecycle management of DoD and Federal information systems. Topics include: principal roles, functional components, and output documents of the C&A process; and a comparison of the government C&A process specification currently in use (DITSCAP/NIACAP, FIPS, DCID 6/3) with the emerging

effort to produce a unified specification. CS-4685 is part two of the two course (CS4680 and CS4685) Certification and Accreditation course sequence. Students will investigate 2-3 case studies of systems that have been evaluated, and then apply the lessons of CS4680 to make final accreditation decisions. Successful completion of this two course sequence leads to NSTISSI DAA and Certifier certification.

The RCEL exercises will generally follow the development guidelines prescribed by DoD. As such, the RCEL network is subject to the DITSCAP just as any operational DoD network. Certification and accreditation students could construct a SSAA (System Security Authorization Agreement) for each configuration of the RCEL.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. COMPUTER SECURITY LEARNING OBJECTIVES ADDRESSABLE IN THE RCEL

A. ACADEMIC AND INDUSTRIAL STANDARDS FOR INFORMATION ASSURANCE

Academia in the U.S. has traditionally followed the recommendations of IEEE (Institute of Electrical and Electronic Engineers) or the ACM (Association for Computing Machines) in setting up educational programs in computer science.

Unfortunately, there is no generally accepted standard for computer security education. In fact, except as integrated into the ACM/IEEE [COM03] guidelines, there are no published standards for computer security education at any academic level.

There are several published standards specific for *training* in information security. Among the most useful are the National Security Telecommunications and Information Systems Security Instruction (NSTISSI) standards:

- NSTISSI No. 4011 - National Training Standard for Information Systems Security (INFOSEC) Professionals, dated 20 June 1994
- NSTISSI No. 4012 - National Training Standard for Designated Approving Authority (DAA), dated August 1997
- NSTISSI No. 4013 - National Training Standard for System Administration in Information Systems Security, dated August 1997
- NSTISSI No. 4014 - National Training Standard for Information Systems Security Officers (ISSO), dated August 1997
- NSTISSI No. 4015 - National Training Standard for Systems Certifiers, dated December 2000

Other *training* standards exist for computer security. The most widely recognized is CISSP (Certified Information System Security Professional) managed by $(ISC)^2$ (https://www.isc2.org/cgi-bin/index.cgi). CISSP has categorized computer security into 10 domains:

1. Access Control Systems and Methodology
2. Applications and Systems Development

3. Business Continuity Planning

4. Cryptography

5. Law, Investigation and Ethics

6. Operations Security

7. Physical Security

8. Security Architecture and Models

9. Security Management Practices

10. Telecommunications, Network and Internet Security

The ISC^2 and other commercial entities provide training to the CISSP standard and categorize their courses by these domains. The CISSP standards are intended to apply strictly at a practical, commercial level. Therefore, theory of operating systems, automata, formal methods and other more academically oriented topics are not included.

Each of the above organizations provides guidance in developing training courses. The focus areas and demarcations between topics provided by each is helpful in developing courses and creating learning objectives for IA training.

A learning objective is a brief, clear statement of what the student should achieve as a result of some learning activity. It should link the learning to successful completion of assigned tasks. A well-written learning objective is specific and measurable. It forms the basis for the training and evaluation. Learning achieved in laboratory-based activities enhances student retention and comprehension [DAL01]. Hill Carver et al. [HIL01], stated:

> The use of [a] dedicated security laboratory as a mechanism for supporting active learning was very beneficial. Without exception, the black teams report that the ability to implement and attempt penetrations elevated their learning above that possible with lectures.

Further supporting this viewpoint, Irvine [IRV01] stated:

> The educational process (for computer security) will be a mix of theory and practice, lecture and lab, so a class might consist almost

entirely of laboratory exercises or have very few. Certain concepts lend themselves to laboratory exercises, while others are best taught at the blackboard.

When designing courses, instructors use many methods to develop comprehensive learning objectives. An important concept in designing learning objectives is to keep the knowledge and experience level of the students clearly in focus. Older[OLD01] proposed an outcome-based model, "No single curriculum can possibly address all of Information Assurance: concentrating on the desired educational outcomes helped us determine how to structure our program." When designing courses, both the current level of expertise and the desired level are critical. The learning objectives must collectively indicate how the student reaches the next higher level.

Learning objectives are achieved through student activities. For this work, we are specifically interested in those activities that take can place in the RCEL environment. In the next section, an examination of those activities is presented.

B. LEARNING ACTIVITIES SUPPORTED IN THE RECONFIGURABLE CYBER-EXERCISE LABORATORY

The RCEL can initially be thought of as an equipment warehouse. Thus, all aspects of creating a network still apply. The only action not undertaken is acquisition. In Figure 6, the three-step DoD life cycle is shown with the more commercially oriented six-step approach super-imposed near the bottom by this author for comparison. The center bar of the figure simply shows that for a DoD system, certification and accreditation activities are on-going throughout the system life cycle.

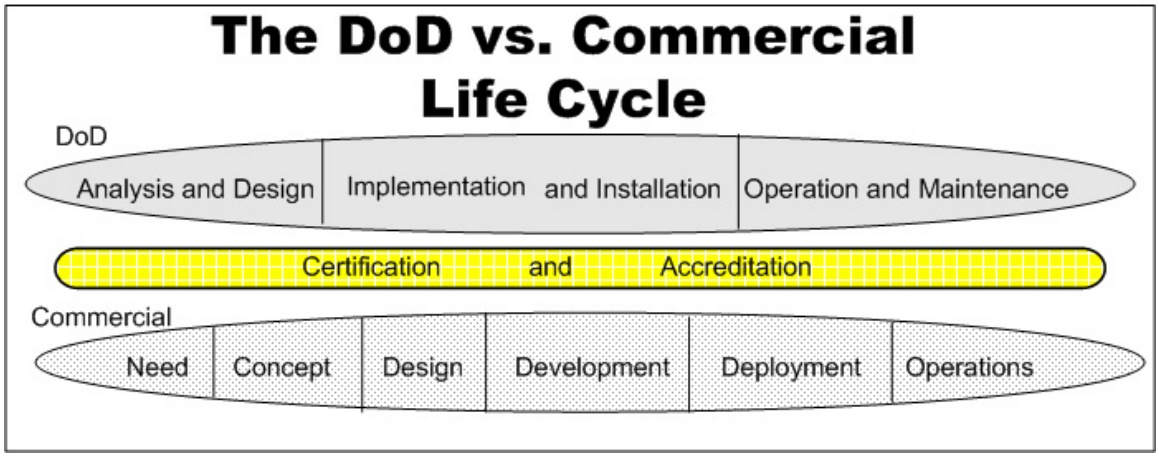

Figure 6. The DoD vs. Commercial Life Cycle

Activities in the RCEL follow the life cycle through all phases. High level activities derived from the RCEL include; needs analysis, concept development, preliminary design, implementation, testing and operation. In addition, the RCEL would include post-existential or post-exercise activities.

For clarification of activities supported in a RCEL, a walk through of a mock inter-scholastic competition exercise might prove useful. In the mock exercise, UoN (University of Nowhere) has asked the Naval Postgraduate School to participate in a cyber defense exercise in the Fall quarter (Oct. to Dec).

The Spring quarter courses begin exercise preparation. Appropriate on-going classes prepare a preliminary RCEL design and assesses the functionality needed. A network security class or equivalent course assesses the security requirements and designs security strategies for the various components. A computer forensics class might prepare the data-collection mechanisms for the lab exercise.

During the summer, the designs prepared by various classes are implemented. When the exercise quarter begins, many classes become involved in preparing and engaging in the exercise. Examples classes (from the NPS curriculum) that may be involved include; Network Security, Network Vulnerability Assessment, C&A, Secure Management of Systems, Computer Forensics, Advanced Topics in Computer Security and Introduction to IA.

At a high level, many learning activities and teaching opportunities took place. Critical thinking and problem analysis were required to solve a set of real challenges. Experiential learning took place in determining the scope of the pending exercise and determining functionality needed. Critical learning activities included: preparing a network design within exercise and equipment constraints, providing network connectivity, optimizing space utilization, etc. Students gained experience creating a security strategy that meets the threat or attack posture posed by the exercise.

When building a network within DoD, all organizations must comply with DoD directive 8500.1 section 5.10.5, which directs heads of DoD components to; “Identify and include IA requirements in the design, acquisition, installation, operation, upgrade or

replacement of all DoD information systems for which they have responsibility." The RCEL at any DoD organization will also be instrumental in instructing students regarding compliance with that directive, and perhaps even to exceed these mandated security minimums. Compliance with DoD directives is assured through certification and accreditation .

There is an opportunity to perform C&A tasks including compliance with DITSCAP (DoD Information Technology Security Certification and Accreditation Process). The C&A students gained experience constructing and maintaining the SSAA (System Security Authorization Agreement) which is the primary documentation demonstrating how the network meet all DoD requirements. Learning took place interconnecting equipment, testing operation and configuring the various physical properties of the network. Exercise participants gained knowledge of implementing and maintaining network services like FTP, DNS, Web, etc.

Experience and learning took place by hardening and testing the systems according to the security plan adopted. Data collection techniques to capture and preserve exercise activities was useful. The forensics students also gained experience analyzing the forensic data gathered. Finally, students gained experience monitoring the operation of a functioning network.

C. SPECIFIC LEARNING OBJECTIVES RELATED TO THE RECONFIGURABLE CYBER-EXERCISE LABORATORY

Teaching of computer security occurs on many levels, see Figure 7. It is instructive as it clearly shows the layers of education in the realm of security. The NPS RCEL is intended for use at a postgraduate school, but there are equally practical applications at the commercial training level as well. The learning objectives in this section can be adapted to coursework at any level. With large aspects of information assurance at the applied level (as is the case for all of computer science), practical aspects of the field are worthy of classroom time.

> The educational outcomes (of security education) must address security needs consistent with the security challenges encountered by graduates in their professional roles. Irvine [IRV05].

The learning objectives presented allow easy creation of evaluation tools (tests) to assess student achievement. A pedagogical note, the learning objectives follow Bloom's taxonomy [BLO02, BLO01] for categorizing learning and learning domains. Bloom's Taxonomy is the generally accepted structure of learning modalities

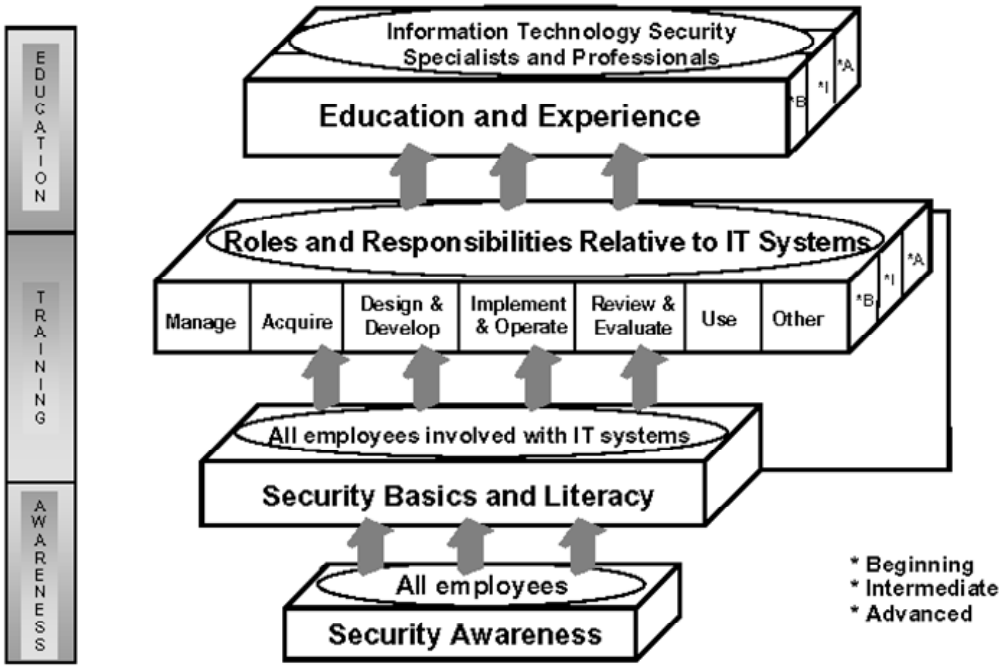

Figure 7. Learning Continuum(from NIST SP800-16 Appendix A)

Table 4. Listing of The Naval Postgraduate School IA Courses

ID	Description
C-1	CS-3600 – IA, Intro to Computer Security
C-2	CS-3670 – IA, Management of Secure Systems
C-3	CS-3675 – Network Vulnerability Assessment
C-4	CS-3690 – Network Security
C-5	CS-4600 – Secure Systems
C-6	CS-4603 – Database Security
C-7	CS-4605 – Security Policies, Models and Formal Methods
C-8	CS-4614 – Advanced Topics in Computer Security
C-9	CS-4677 – Computer Forensics
C-10	CS-4680 & 4685 – Intro to C&A and Case Studies

The reader may freely adopt these learning objectives for courses or training performed at their own RCEL facility. Each learning objective is mapped to one or more NPS courses that was described earlier in this document. The learning objectives are further categorized into five basic areas; computer laboratory skills, networking, analysis, security and leadership.

All of the learning objectives are accomplished in the course of the advanced exercise Scenarios III, IV, V & VI discussed later in this work.

1. Computer Laboratory Skills

LO-1. After completing indoctrination to the RCEL, the student will be able to identify all RCEL stations and describe their functions.

Naval Postgraduate School Courses: C-1, C-2, C-3, C-4, C-8, C-9, C-10

LO-2. After a period of discovery learning, when assigned to a RCEL station, the student will be able to:

a. of the RCEL.Describe the functional significance of the station

b. Implement the function(s) required of the station within the constraints

Naval Postgraduate School courses: C-1, C-3, C-4, C-9

LO-3. The student will learn the correct operation of systems employed in the RCEL and be able to demonstrate that ability.

Naval Postgraduate School courses: C-1, C-2, C-5, C-8, C-10

LO-4. After participation in any phase of the RCEL implementation the student will be able to identify each component of the implemented LAN and be able to relate that component to corresponding layers of the ISO networking model.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-9, C-10

LO-5. After familiarization with the RCEL network, the student will be able to interpret the RCEL network diagrams and verify the presence of each system component.

Naval Postgraduate School courses: C-1, C-2, C-4, C-5, C-6, C-8, C-10

LO-6. After participating in a RCEL exercise, the student will gain an increased knowledge of potential security issues. The student will be able to demonstrate this by articulating possible variations and extensions on her RCEL experiences.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-7, C-8, C-10

2. Networks

LO-7. After receiving introductory training in the RCEL, the student will be able to describe the topology of the RCEL as implemented.

Naval Postgraduate School courses: C-1, C-4, C-10

LO-8. After implementing the network specification for the RCEL the student will be able to discuss the use of VLAN technology and the implications in active networks.

Naval Postgraduate School courses: C-2, C-3, C-4, C-9

LO-9. Given that the student was assigned to the firewall, router or switch station during an exercise, the student will be able to demonstrate a working

knowledge of the operating system interface for the device and articulate the configuration process for these devices

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-10

LO-10. After training in the current configuration of the RCEL the student will be able to articulate the scheme of IP addressing implemented.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-9, C-10

LO-11. After advanced training and practice on actual machines, the student will be able to do security related configuration operations on routers and switches.

Naval Postgraduate School courses: C-4, C-10

LO-12. After a complete exercise the student will be able to recognize the symptoms of a system under attack or one that has been compromised.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-6, C-9, C-10

LO-13. After participating in a RCEL exercise the student will be able to interconnect equipment using Ethernet cabling and be able to identify appropriate jacks, plugs and cable types.

Naval Postgraduate School courses: C-1, C-4

LO-14. After completing the analysis and design of a RCEL topology, the student will be able to describe the AAA(this is Cisco specific, authentication, authorization, and accounting) scheme and articulate how it is implemented.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-6, C-7, C-8, C-9, C-10

LO-15. After a complete exercise the student will be able to discuss and articulate such networking concepts DHCP, PDC/BDC, DNS, VLAN, etc., and how each is manifested in the current configuration.

Naval Postgraduate School courses: C-1, C-2, C-4, C-6, C-10

LO-16. Before beginning work in the RCEL but after some appropriate classroom training, the student will demonstrate an understanding of VPN technology.

Naval Postgraduate School courses: C-1, C-4

LO-17. After appropriate instruction the student will be able to demonstrate in the RCEL proficiency and correct analysis of the results obtained using rudimentary networking tools such ping, trace route, etc.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4

LO-18. The student will be able to correctly interpret results obtained in the RCEL when using network tools such as ping, trace route, nslookup, etc.

Naval Postgraduate School courses: C-1, C-3, C-4, C-9

3. Security

LO-19. Upon completion of a RCEL exercise the student will be able to:

a) analyze vulnerability exploits used

b) discuss their effectiveness

c) interpolate how these exploits might affect a “real” network

d) prioritize the risks and vulnerabilities of the system

Naval Postgraduate School courses: C-1, C-3, C-4, C-7, C-8, C-10

LO-20. At the conclusion of a RCEL exercise the student will be able to analyze and evaluate the security plan that was implemented and recognize the strengths and weaknesses of that plan.

Naval Postgraduate School courses: C-4, C-6, C-10

LO-21. After appropriate coursework in IA, the student will be able to detail the security requirements for an implementation of the RCEL.

Naval Postgraduate School courses: C-1, C-2, C-3, C-4, C-6, C-9, C-10

LO-22. Given a security plan for the RCEL, the student will be able to assess the plan and take an active role in the implementation of the plan.

Naval Postgraduate School courses: C-4, C-10

LO-23. Upon completion of the RCEL design the student will be able to discuss the defensive posture of the proposed network design.

Naval Postgraduate School courses: C-4, C-10

LO-24. Upon completion of the design and implementation of the network the student will be able to demonstrate and discuss each of the four areas of security present in the RCEL; confidentiality, integrity, authenticity and availability.

Naval Postgraduate School courses: C-1, C-4, C-10

4. Analysis

LO-25. After participating in a RCEL exercise the student will be able to recognize and describe obvious security flaws in the network design.

Naval Postgraduate School courses: C-4, C-8, C-9, C-10

LO-26. When the RCEL is used in conjunction with the computer forensics course, the student will, upon completion of an exercise, be able to perform basic forensic analysis on compromised systems.

Naval Postgraduate School courses: C-4, C-9

LO-27. The student will be able to discuss how to translate her experience into real network environments.

Naval Postgraduate School courses: C-4, C-10

LO-28. After implementing a RCEL design the student will be able to articulate how cryptography is used in the network.

Naval Postgraduate School courses: C-1, C-8, C-9

5. Leadership

LO-29. After managing a RCEL station through an exercise scenario, the student will be able to analyze, test and confirm the functionality of that station.

Naval Postgraduate School courses: C-2, C-3, C-4, C-7, C-9, C-10

LO-30. Upon completion of the design phase of a RCEL exercise the student will be able to develop an implementation plan describing the activities needed to complete the implementation.

Naval Postgraduate School courses: C-8, C-10

LO-31. Upon completion of the design phase of a RCEL exercise the student will be able to demonstrate that the final design meets the exercise requirements.

Naval Postgraduate School courses: C-10

LO-32. Prior to initiating an exercise, the student will be able to assess the readiness of the network and specifically the stations to which they are assigned.

Naval Postgraduate School courses: C-4, C-5, C-7, C-8, C-10

LO-33. Upon completion of an exercise the student will be able to verify the utility of pre-existing network security checklists.

Naval Postgraduate School courses: C-4, C-10

LO-34. After implementation of a RCEL topology the student will be able to discuss the process of implementation and articulate mistakes that were made, delays that were suffered and ways the process might be improved.

Naval Postgraduate School courses: C-10

LO-35. After familiarization with the RCEL and in conjunction with the secure management of systems class the student will be able to assess the security and business continuity posture of the current topology.

Naval Postgraduate School courses: C-2, C-10

LO-36. Upon completion of any phase of the RCEL lifecycle the student will be able to discuss team leadership and articulate learning related to team management and conduct.

Naval Postgraduate School courses: C-10

LO-37. After completing a RCEL exercise, the student will be able to read, interpret and manage the implementation of a network security plan.

Naval Postgraduate School courses: C-10

THIS PAGE INTENTIONALLY LEFT BLANK

V. EXAMPLE CYBER-EXERCISE SCENARIOS

The primary function of the RCEL is to provide an enabling technology for inter-organization training and cyber defense exercises. In this chapter, six possible scenarios are created. In designing each scenario and the associated network topology, design principles first codified by Saltzer and Schroeder [SAL01] in their 1975 paper on computer protection are used. Those principles, quoted here from the 1975 paper, are :

- Economy of Mechanism: The protection mechanism should have a simple and small design.
- Fail-safe Defaults: The protection mechanism should deny access by default, and grant access only when explicit permission exists.
- Complete Mediation: The protection mechanism should check every access to every object.
- Open Design: The protection mechanism should not depend on attackers being ignorant of its design to succeed. It may however be based on the attacker's ignorance of specific information such as passwords or cipher keys.
- Separation of Privilege: The protection mechanism should grant access based on more than one piece of information.
- Least Privilege: The protection mechanism should force every process to operate with the minimum privileges needed to perform its task.
- Least Common Mechanism: The protection mechanism should be shared as little as possible among users.

As each scenario is developed and a network designed and built, a security plan will need to be developed. Creating a security plan is difficult and time consuming. Often, it is best to use a guide or template and tailor it to the specific needs of the network being protected. Extensive research has not turned up a better general guide for building a security plan than the template provided by NIST. In Appendix C the NIST template for security plans for both major application and general support systems is presented.

Reconfiguring the RCEL for alternate scenarios involves a specific set of tasks. It is likely that changing scenarios also means changing equipment, software, people and connections. This may entail additional, unplanned activities. For example, when one

group of students finishes a scenario exercise, the next group may discover the passwords to the routers and switches are no longer available. Most router and switch passwords can be reset or recovered if the operator is familiar with the proper techniques and has physical access to the devices. Resetting lost passwords on Cisco routers [CIS04] takes only a few minutes, but involves being able to cycle the power and connect a terminal to the device so a configuration register can be reset.

Another issue is upgrades to operating systems and applications. Doing upgrades between exercises is ideal. When an exercise is in progress and the network completely isolated upgrades are far more difficult. A related issue is licensing. Before deploying a new configuration the area manager must be sensitive to any licensing issues.

Of course the most serious and critical issues relate to network security. It is imperative that all connections are checked. Verify that the RCEL is not accidentally or covertly connected to the internet.

Each scenario will include a design, a set of activities, and an appropriate network configuration. For each exercise, chronological lists of activities are provided. Each activity has a list of the appropriate references and an additional reference to the appropriate learning objectives defined in chapter IV. To assist the reader, the L.O.s are further designated G, N, S, A or L (General Skills, Networking Skills, Security, Analysis or Leadership, respectively) according to the category in which they are found. For example, 1G, is learning objective 1, General Skills. Since the L.O.s are themselves cross-referenced to NPS courses, it is now possible to trace an activity in the RCEL to a learning objective, a useful reference, and an appropriate class. There is, of course, a great deal of overlap.

A. SCENARIO I - LOCAL ONLY

1. The Design

In this scenario no outside organization is involved. The VPN is inactive and the RCEL is effectively air-gapped form any Internetworking connectivity.

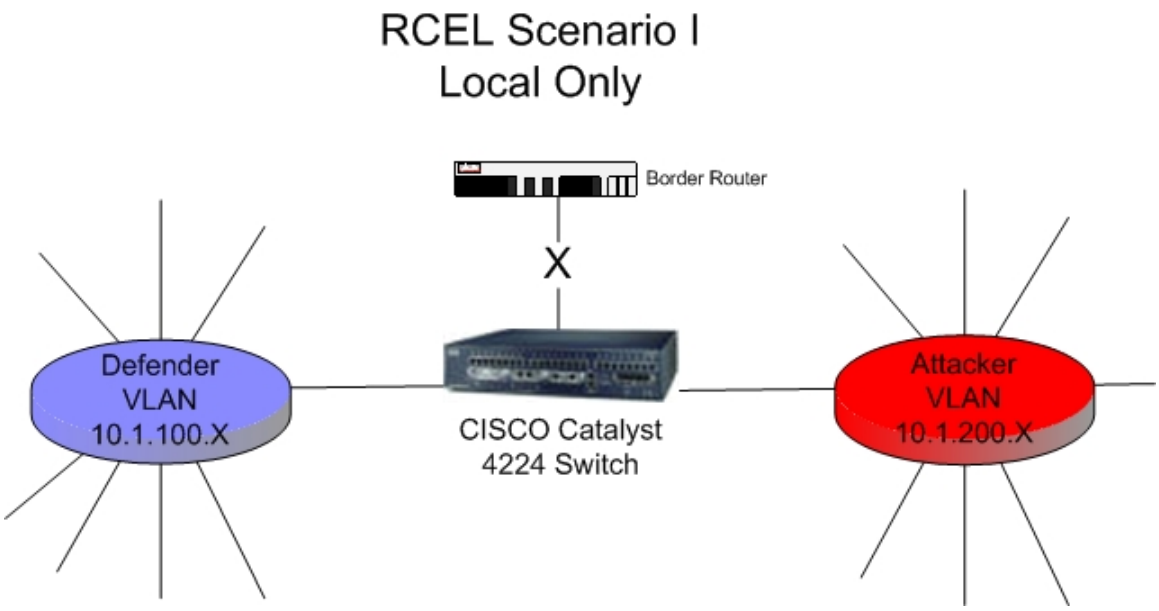

Figure 8. Scenario I Configuration

Figure 8, depicts a simple scenario. When the RCEL is operated in this way, the connection to the border router (and VPN) is disconnected. An effective way to configure the network may be using VLAN technology. Here the central switch, the Cisco 4224, 'becomes' the "internet," providing routing and interconnectivity between the networks.

Each of the areas, attacker and defender, are configured as VLANS. Configuring VLANs on the Cisco router is relatively easy. In Figure 9, the concept of two VLANs connected to a single switching element is shown. In Scenario I, we disregard the connection to the router which has been disabled or turned off. A router interface can be disabled with the IOS command: *Router(config-if)# shutdown.*

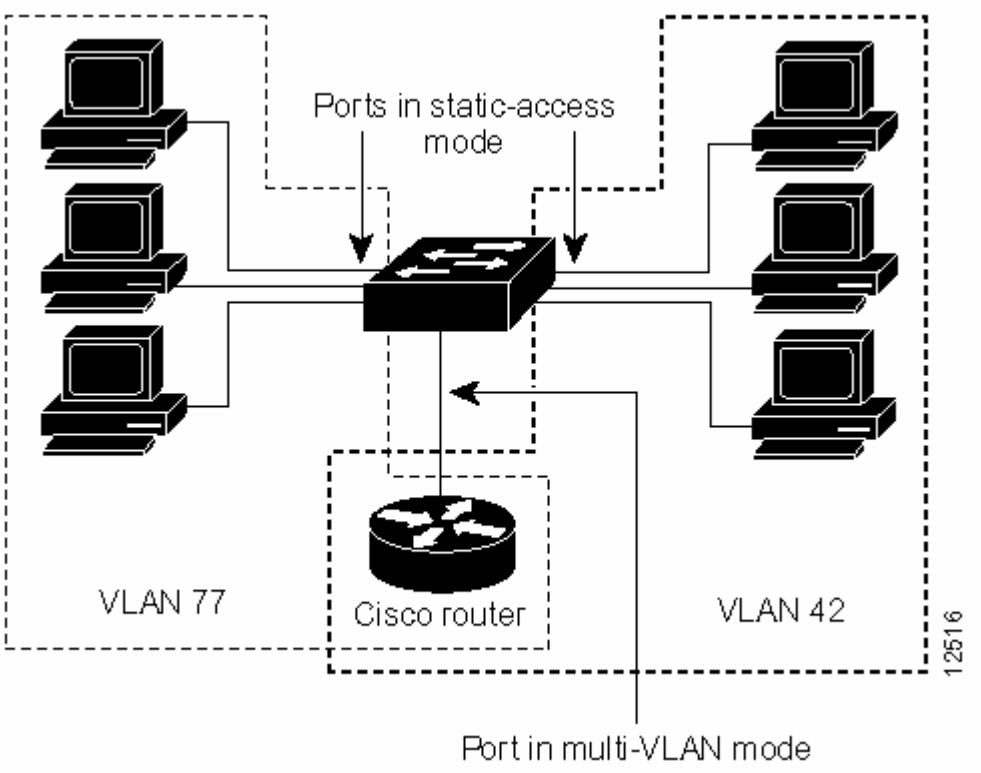

Figure 9. VLAN conceptual diagram from the Cisco Online Documentation (CDROM)[CIS01]

Figure 9 shows three computers on each VLAN, but there could be as few as one, or as many as desired, constrained only by the maximum number of hosts that the switch can manage.

To create a Vlan, use the IOS command: "set Vlan Vlan-num Vlan-name." Thus, the command: set Vlan 77 defender, would create the Vlan with number 77 and the name "defender." Once the VLANs are created and properly configured, (See Cisco Online Documentation for all Cisco references and suggested configurations) the switch's currently running configuration file will contain an entry similar to:

```
interface Vlan 77
ip address 10.1.100.1 255.255.255.0
ip access-group 101 in
ip access-group 102 out
interface Vlan 42
ip address 10.1.200.1 255.255.255.0
```

```
ip access-group 102 in
 ip access-group 101 out
```

Note in the listings above, the lines that refer to IP access-groups. These lines refer to access lists, specifically access lists 101 and 102 which provide layer 3 and/or 4 filtering at the switch. The exact content of such lists would be based on the specific network and would be created at the time the VLAN is configured. The applied access lists control the type of packets permitted or blocked at the VLAN interface (either in-bound or out-bound) by selecting packets for filtering based on source or destination address, port number, protocol, connection state and packet fragmentation. This capability further strengthens the VLAN by providing isolation and protection specific to the needs of that network segment.

These configuration entries reflect the creation of two VLANs, 77 and 42. Cisco VLAN numbers are restricted to numbers between 2 to 1001. Other numbers are reserved for use by other functionality of the switch.

Once the VLANs exist, the switch's physical ports, into which the computers are connected with standard Cat5 RJ45 terminated cables, must be associated with the appropriate VLAN. The configuration entries below reflect that physical ports 22, 23 and 24 on the switch are associated with VLAN 77. The line "switchport access vlan 77" shows the association. The line "interface FastEthernet5/22" identifies physical port 22 on module 5 that will have one of the computers plugged into it. Each port would have a configuration script similar to:

```
interface FastEthernet5/22
 no ip address
 duplex auto
 speed auto
 switchport access vlan 77
 snmp trap link-status
 no cdp enable
```

In a like manner, ports 19, 20 and 21 on module 5 will be associated with VLAN 42. The switch needs little other configuration beyond the normal administrative tasks. IP address filters, ACLs, etc., will vary with each organization and exercise. The intent

of this work; however, is not to teach Cisco switch configuration, but to demonstrate a possible configuration for Scenario I. A source of information is the Cisco configuration guides which can be found at:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/.

The physical interconnections allow the PCs to send packets to the network (see the appropriate documentation for the PC or device in use) and to the appropriate port/VLAN of the switch.

Looking at the attacker LAN, the activities of the attacker will most likely follow a distinct pattern. Such as that outlined by McClure [MCC01].

2. RCEL Activities for Scenario I

So, the activities of this scenario for the attacker are:

1. Define the needs of the attacker side of the LAN [MCC01, NAT17, MAN01]
   {L.O.s: 6G, 11N, 14N, 15N, 17N, 18N, 19S, 20S, 21S, 23S, 24S, 25A, 27A, 28A, 31L, 32L, 34L}
2. Connect the hardware [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01]
   {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}
3. Configure and test the VLAN on the switch [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01]
   {L.O.s: 5G, 7N, 8N, 10N, 14N, 15N, 17N, 18N, 22S, 23S, 27A, 30L, 31L 32L, 33L, 34L, 36L, 37L}
4. Configure and test the workstations [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]
   {L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

5. Define the attack goals and formulate an attack plan [MCC01, MAN01]
   {L.O.s: 1G, 4G, 5G, 6G, 9N, 14N, 15-18N, 19-24S, 25-28A, 30L, 33L, 34-37L}
6. Acquire the “hacking” tools and exploits needed [MCC01]
   {L.O.s: 6G, 12N, 14N, 19S, 24S, 25-28A, 30L,33L, 34-36L}
7. Engage in the attack following McClure’s 9 steps [MCC01]
   {L.O.s: 3G, 4G, 6G, 7-18N, 19-24S, 25-28A, 33-36L},
8. Disengage the attack[MCC01, LAR01, NAT17, DAY01, KEL01]
   {L.O.s: 12N, 13N, 17N, 34L}
9. Analyze the success/failure of the techniques and tools employed[DEP02, MAN01, DAY01]

   {L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

Looking back at the learning objectives, this scenario accommodates all of the learning objectives listed in Chapter IV, although in a more limited way. Due to the limited scope and small scale of this scenario, some L.O.s are covered in far more depth than others.

Now let’s look at the defender VLAN. Major activities on this side are:

1. Define the defensive needs of the network [SAN01, DEP02, FRA01, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}
2. Write a security plan [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT12, NAT04, KEN01, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}
3. Configure the VLAN on the switch [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01]

{L.O.s: 5G, 7N, 8N, 10N, 14N, 15N, 17N, 18N, 22S, 23S, 27A, 30L, 31L 32L, 33L, 34L, 36L, 37L}

4. Connect the hardware [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17,ROS01]
   {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}
5. Configure, connect and test the workstations including security [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01,KEL01, GER01]

   {L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}
6. Implement and test the security plan including incident response and operational continuity [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT13, NAT12, NAT04, KEN01, NAT17, DAY01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16-18N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

7. Defend the net [SAN01, IRV01, HIL01, BIS01, MAY01, NAT18, COM02, PFL01, NAT15, NAT16, NAT12, NAT03, NAT06, NAT10, LIT01, RUS01, MCC01, FRA01, NAT17, MAN01, LON01, ROS01, KEL01]

   {L.O.s: 3-6G, 7-18N, 21-24S, 26A, 28A, 29-37L}
8. Disengage the exercise [MCC01, LAR01, NAT17, DAY01, KEL01]
   {L.O.s: 12N, 13N, 17N, 34L}
9. Analyze the success/failure of the security plan [FRA01, NAT17, MAN01]

   {L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

10. Analyze (forensically) any penetrations or collected evidentiary data. [MCC01, FRA01, NAT17, MAN01]

    {L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L}

Scenario I is closely akin to a traditional lab exercise. This network may be configured in a day, the remaining aspects of the scenario done in a day or over a period of a week or more.

VLANs allow this scenario to be on-going while other activities are taking place on the switch. The Cisco 4224 used in the Naval Postgraduate School RCEL, is a 24 port switch. Allotting 6 ports to this scenario allows four separate Scenario I activities to take place simultaneously.

B. SCENARIO II - LIMITED INTERACTION DEFENSE ONLY

1. The Design

This scenario provides a defensive exercise configuration. Configure the RCEL to appear as a "normal" small organization's network. In this exercise, a minimal amount of equipment is set up. The RCEL network is hardened according to a pre-existing security plan [DEP01, NAT15, NAT16, NAT12, NAT10, RUS01]. But it is not too well hardened, however, since we actually want the attacker to succeed. Successful attacks enable defenders to watch and record the attack and the progression of penetration and compromise. A great deal of experiential learning comes from being the victim of an attack [BIS01, MAY01, DAL01] (in a controlled environment).

An agreement is made between the defending RCEL (blue team) and an external organization that will act as the attacker (red team). This may be another school, another department, the local hacker's club, or perhaps someone as able and sophisticated as the NSA or CIA. The external organization then attacks the RCEL network and tries to gain access, acquire information (e.g., "capture the flag"), or disrupt operation. This may involve the use of malware, back doors, denial of service, interception or any other attack technique. The limitations of the attack will be set in advance by agreement between the defending side administrator and the attacker organization.

In this scenario, the VPN connects to the attacker and serves as the access gateway for the network. The first router is located behind a hub (see Figure 10 below) allowing for an Intrusion Detection System (IDS) station to electronically monitor all network traffic. The attacker is forbidden from attacking the data collection laptop (if detected) but the IDS is fair game. The data collection laptop is used by an instructor or manager to monitor network activities or record raw traffic.

The Scenario II configuration of the RCEL includes a router, a firewall, a switch, an application server, a web server and a syslog server. Note, there is no DMZ and no mail server. The application server may be running any application appropriate to the exercise or agreed upon by the exercise participants. Of course, the participants may add features or servers as necessary to meet specific requirements.

When deploying an IDS [CIS03], the specific implementation must be tuned for maximum effectiveness and to reduce false positives caused by legitimate traffic. In Figure 10, the IDS is configured as a Network Intrusion Detection System (NIDS) versus a Host-based Intrusion System (HIDS). When a threat is detected the IDS provided passive notification to the administrator or other agent per the specified configuration. The choice of response is dependent upon the goal of the network security plan. A NIDS that only records and quietly alerts can be thought of as a "silent alarm."

Configuring a NIDS requires careful consideration and planning. In this exercise, we are only interested in detection. That is, it will be more important to allow some attack traffic in than to automatically "shun" or filter any hosts detected as the origin of the attack. This may be true in some operational networks as well.

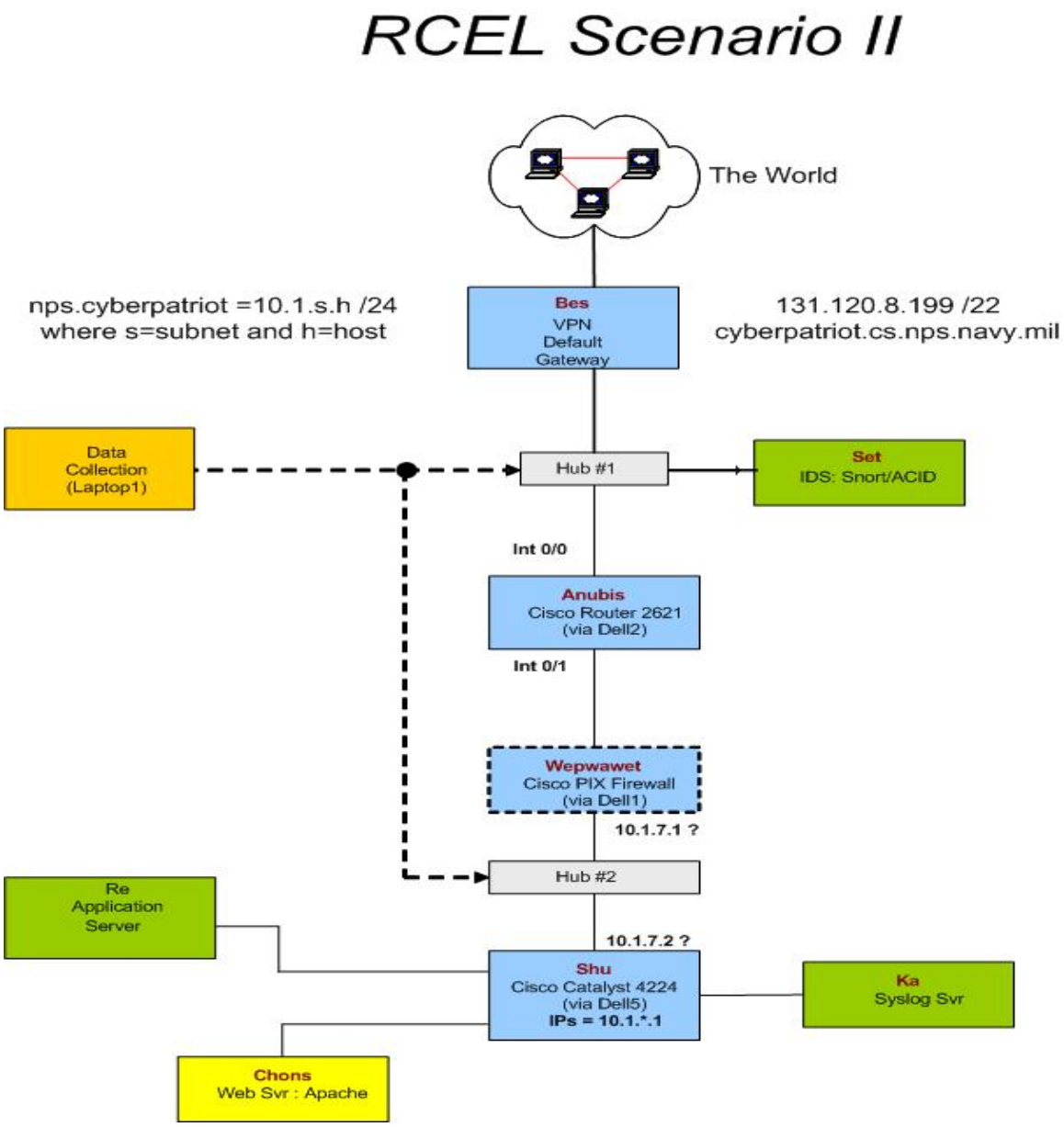

Figure 10. Scenario II - Defense Only

The Cisco Pix firewall, along with the router filters form the primary perimeter defense of the network. This exercise assumes an attacker will attempt penetration, however, a reasonable but soft perimeter defense should be in place initially to provide educational strength and completeness to the exercise. If the attacker fails to penetrate the perimeter after some previously negotiated timeframe, the perimeter defense will be reduced further or removed to allow penetration.

2. Network Design Elements

The most critical aspect of Scenario II (and also Scenarios III, IV, V and VI) network is the use of the VPN to connect to the external organization. VPNs use several technologies including PPTP (Point to Point Tunneling Protocol), L2TP (Layer Two Tunneling Protocol), or even SSL (Secure Socket Layer) and SSH (Secure Shell). Each technology has pros and cons. Today's more robust VPN appliances and software, like the Cisco Pix-506 used in the NPS RCEL, support IPSec.

Of all the VPN technologies available, IPSec is the technology of choice for the support of RCEL exercises wherein the opposing networks are connected across a shared, public network. The reason for this is twofold. First, IPSec is employed at the network layer; thus every application that participants may want to involve in any particular exercise scenario can be encapsulated in the encryption tunnel as the application payload (OSI layer 7) is passed down to the IPSec (OSI layer 3) processing module. Second, when employed in tunnel mode on a gateway machine that serves as the only link between the RCEL network and the external public network, IPSec will leave all of the original RCEL machines' IP information intact, and simply encapsulate the traffic in a new IP header. Such usage of IPSec in tunnel mode provides both packet encryption and network address translation (NAT) for the private IP space that is likely being used in the RCEL.

IPSec [KEN01, VPN01] technology as described in RFCs 2401, 2406, 2407, 2408, 2409, 2547, and 3193 allows for the establishment of an encrypted "tunnel" or connection between hosts. RFC-2401 defines IPSec as:

> IPsec provides security services at the IP layer by enabling a system to select required security protocols, determine the algorithm(s) to use for the service(s), and put in place any cryptographic keys required to provide the requested services. IPsec can be used to protect one or more "paths" between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. (The term "security gateway" is used throughout the IPsec documents to refer to an intermediate system that implements IPSec protocols. For example, a router or a firewall implementing IPsec is a security gateway.)

Note that anyone attempting to set up a VPN must familiarize themselves with all pertinent RFCs and the documentation provided by the manufacturer of the VPN products in use.

An excellent reference for VPN information is the VPNC (VPN Consortium, http://www.vpnc.org). The VPNC defines three types of VPN technologies[VPN01]; Secure VPN, Trusted VPN, and Hybrid VPN. The RCEL must use a secure VPN technology. Secure VPN technologies include IPsec with encryption in either tunnel or transport mode or IPsec inside layer 2 tunneling protocol (L2TP as described in RFC-3193). The exact manner in which the VPN is established depends entirely on the software or hardware used. Some VPN systems have very nice GUI interfaces that allow the administrator to point and click all the settings necessary. On the other end of the spectrum are the command line systems requiring a thorough knowledge of the product and VPN technology to correctly configure.

In the RCEL, the VPN station is critical and must be assigned to people who are interested, knowledgeable (or want to become so) and can be trusted to respect the seriousness and importance of this duty.

In the network diagram shown in Figure 10, a second hub is located between the firewall and the switch. This is considered “invisible” to the network and is used only to permit sniffing, monitoring and other vulnerability assessment and exercise specific activities.

Within the network, tools like TripWire can be deployed. Tripwire (an open source solution) monitors changes to files residing on Linux systems (the commercially available version works on Unix and Windows). The program detects changes in key attributes of files that should not change, including binary signature, size, etc. Commercial versions are available.

Nessus is a publicly available tool that monitors and checks for security vulnerabilities on a network. More information can be found at http://www.nessus.org. It is a good idea to put a sniffer in place as well. A good sniffing product that is freely

available is Ethereal (http://www.ethereal.com). This tool lets the user see incoming packets in real time and dissect them into their component parts for easy reading.

There is significant debate in the IA community about the value of IDS and the role it should play in overall security. It is not within the scope of this work to solve this debate, only to make the reader aware. IDS can be simplistic (a sniffer) or more sophisticated as in the Cisco IDS 4250 Appliance Sensor. The Cisco marketing literature claims the IDS-4250 "raises the performance bar for high-throughput gigabit protection in a performance-upgradeable IDS chassis." The importance of the IDS and sniffer to the RCEL is student awareness and familiarity.

In Figure 11, a capture of a small part of a session is shown. The highlighted line in the top area selects a particular packet. In the middle area, the packet's structure is broken out and in the lower segment the hex is highlighted that relates to the particular protocol selected in the center frame. With this tool, users quickly see what is coming into the network and what ports and protocols are in use or requested.

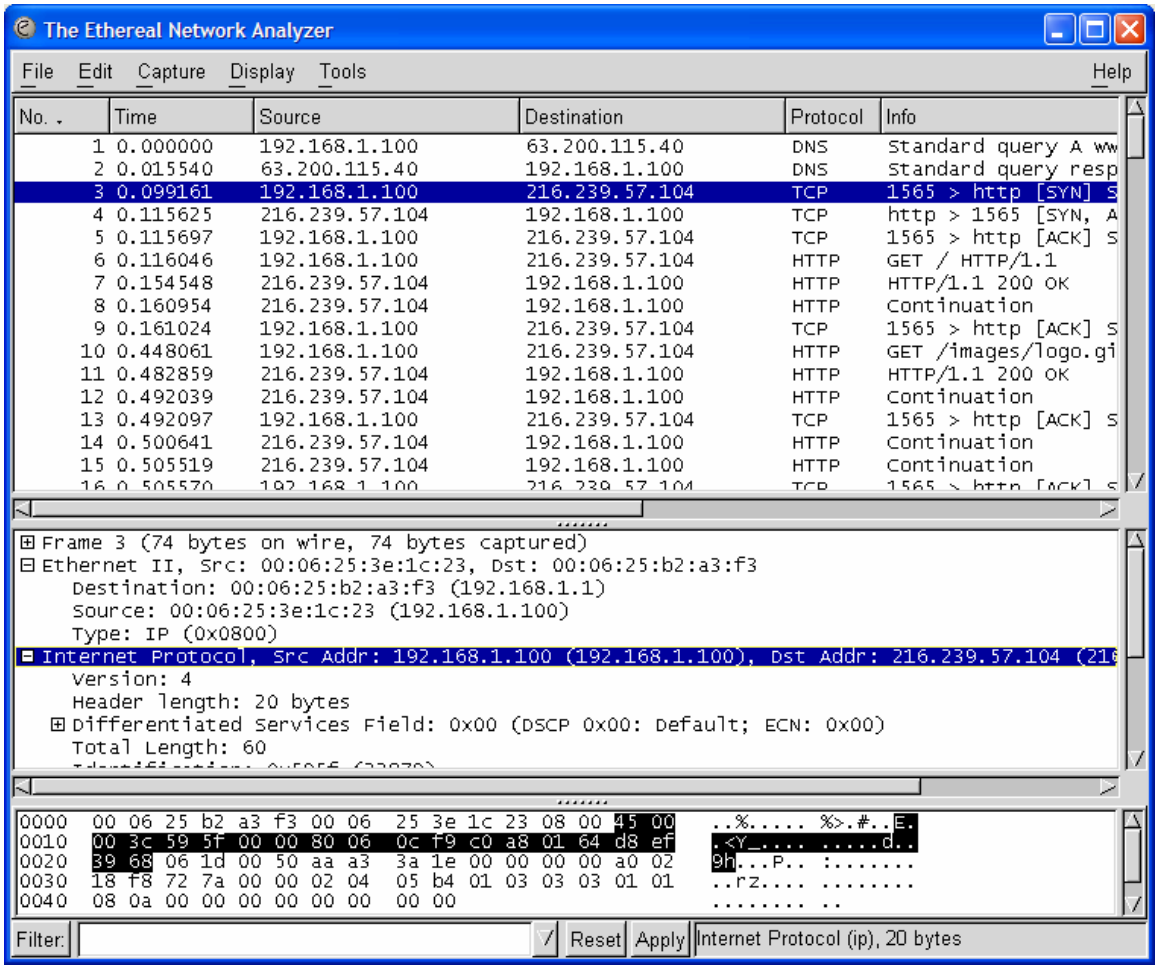

Figure 11. Ethereal Capture

3. RCEL Activities for Scenario II

The activities associated with this configuration are similar to those in Scenario I for the defender side with some additions.

1. Define the needs and scope of the network IAW the planned exercise [IRV03, HIL01, LAN01, BIS01, MAY01, 42, MCC01, MAN01, HOF01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

2. Write a security plan [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT12, NAT04, KEN01, NAT17]

{L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

3. Connect the hardware (without connecting the VPN to the internet or the router) [COM02, CIS01, DEF01, NAT12, NAT04, NAT08, LAR01, NAT17, ROS01, LEI01]

4. {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}

5. Configure the switch as needed [CIS01, LAR01, LON01]

   {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

6. Configure and test the workstations including security per the security plan [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]

   {L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

7. Implement and test the remainder of the security plan including incident response and operational continuity [SAN01, NAT13, NAT17, DAY01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16-18N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

8. Implement and test the vulnerability assessment and IDS stations [NAT06]

   {L.O.s: 2G, 4G, 6G, 12N, 14N, 20S, 23S, 24S, 28A, 29L, 34L, 37L}

9. Configure the VPN according to the security plan and the requirements of the local network administrator [CIS01, KEN01, LAR01]

{L.O.s: 1G, 4G, 5G, 7N, 9N, 10N, 11N, 14-18N, 23S, 24S, 27A, 28A, 29-34L}

10. Test the VPN with the attacking organization without the RCEL router connected [CIS01, KEN01, LAR01]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L}

11. Connect the RCEL router when the exercise is ready to begin [NAT12, ELE01]

    {L.O.s: 2G, 6G, 9N, 10N, 13N, 15-18N, 23S, 24S, 29L, 31L, 32L, 36L}

12. Test the security of the VPN [CIS01, KEN01, LAR01, NAT17]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L, 37L}

13. Conduct the scheduled exercise [SAN01, IRV01, HIL01, BIS01, MAY01, NAT18, COM02, PFL01, NAT15, NAT16, NAT12, NAT03, NAT06, NAT10, LIT01, RUS01, MCC01, FRA01, NAT17, MAN01, LON01, ROS01, KEL01]

    {L.O.s: ALL}

14. Collect data during the exercise [MAN01]

    {L.O.s: 3G, 4G, 5G, 9-12N, 14N, 15-18N, 19-24S, 29L, 32L, 35L}

15. Disconnect the router and VPN when the exercise is concluded[CIS01, KEN01, LAR01]

    {L.O.s: 8N, 12N, 13N, 17N, 18N, 19S, 23S, 25A, 27A, 33L, 34L, 36L}

16. Analyze the success/failure of the security plan [FRA01, NAT17, MAN01]

{L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

17. Analyze (forensically) any successful attacks. [MCC01, FRA01, NAT17, MAN01]

{L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L}

In Scenario II, all learning objectives for the RCEL are available to instructors and students except those specifically related to attack techniques. This scenario is an excellent way to start a RCEL and to safely demonstrate the virtues of this type of education with minimal risk of some unfortunate incident taking place. This scenario can be exciting, interesting and challenging. If the attacker is very sophisticated, the scenario is enhanced.

This exercise must provide dynamic latitude in defensive implementations as it is actually desirable that the attacker penetrate the defended system at some point during the exercise so the students can gain the experience. Thus, if the defense is so well implemented the attackers cannot penetrate, the defenders should soften it as the exercise progresses until the it is ultimately penetrated.

C. SCENARIO III – LIMITED INTERACTION ATTACK ONLY

1. The Design

In the opposite of Scenario II, students assume the role of attacker in Scenario III. Students learn a great deal about defending a network when they understand how attacks are mounted and carried out. Training students to conduct attacks prepares them for performing vulnerability analysis is beneficial for organizations charged with such tasks. In Figure 12 we see an attack configuration. Just as a hacker or group of hackers is not seriously concerned with the victim attacking in response, this configuration allows the red team (attackers) maximum freedom and minimum impedance from security measures. Note, there is no firewall, no IDS, no VLANs, no authentication and so on.

To attempt this configuration in a normal lab is very difficult because the local network's security and restrictions inhibit many attacks and the use of malware. .

Attackers should formulate an attack plan [MCC01] and go about gathering tools to carry out that plan. Some attack methods will be novel, but most will come from

existing sources such as “hacker” web sites. One such site, “The Cult of the Dead Cow” (http://www.cultdeadcow.com) is quite useful. Caution must be exercised when visiting these sites to prevent introducing malware into the research machine.

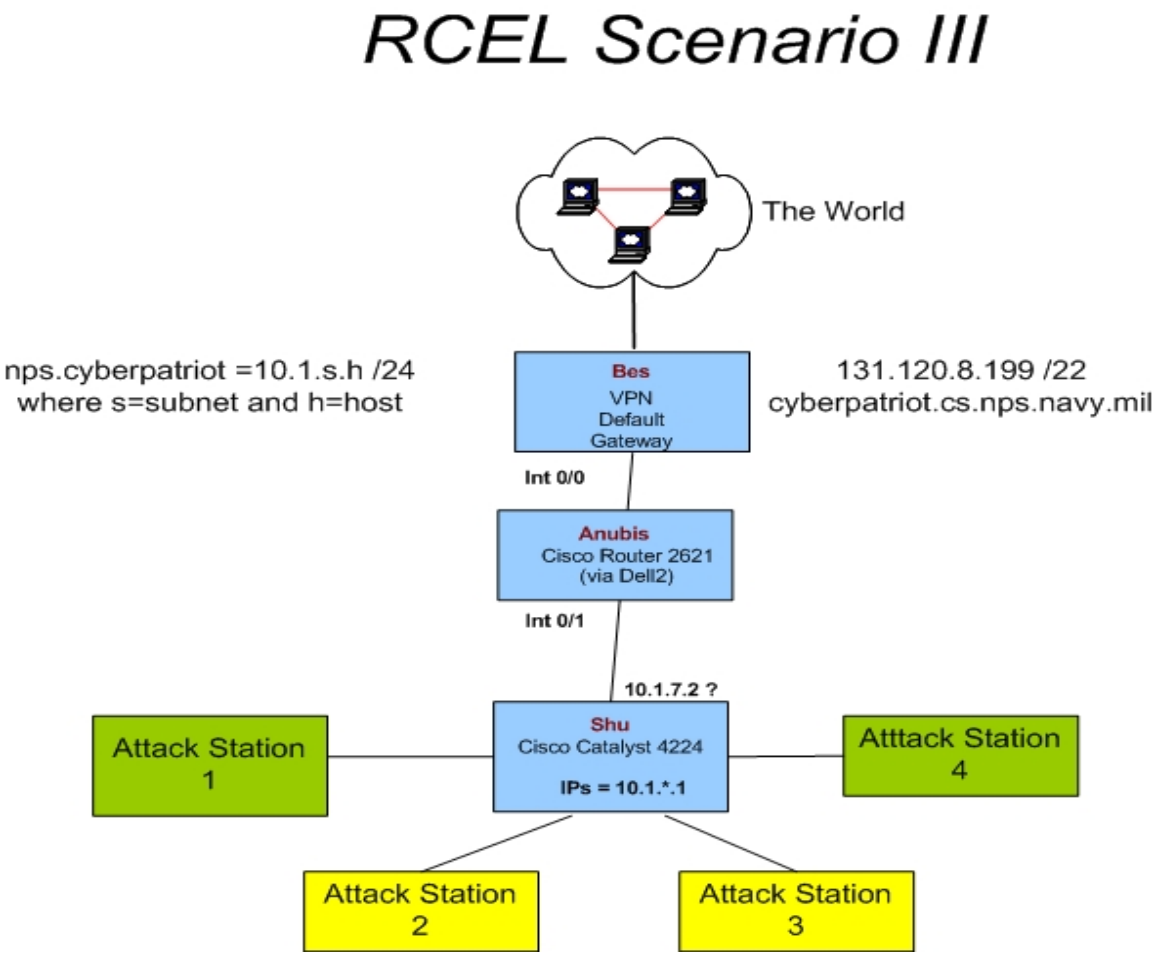

Figure 12. Scenario III - Attack Configuration

More reputable web sites for collecting tools include http://www.insecure.org, http://www.blackhat.com, http://www1.corest.com, http://www.sans.org, http://icat.nist.gov, http://www.hacker-tools.com and many more.

Primary among the tools needed is Nmap. Nmap can be freely downloaded from insecure.org. There is a command line version and a GUI version. This tool is used to map a network’s machines and open ports. The documentation for Nmap states, “*Nmap* is designed to allow system administrators and curious individuals to scan large networks

to determine which hosts are up and what services they are offering." (http://www.insecure.org/nmap/data/nmap_manpage.html). Red Team members are "curious individuals."

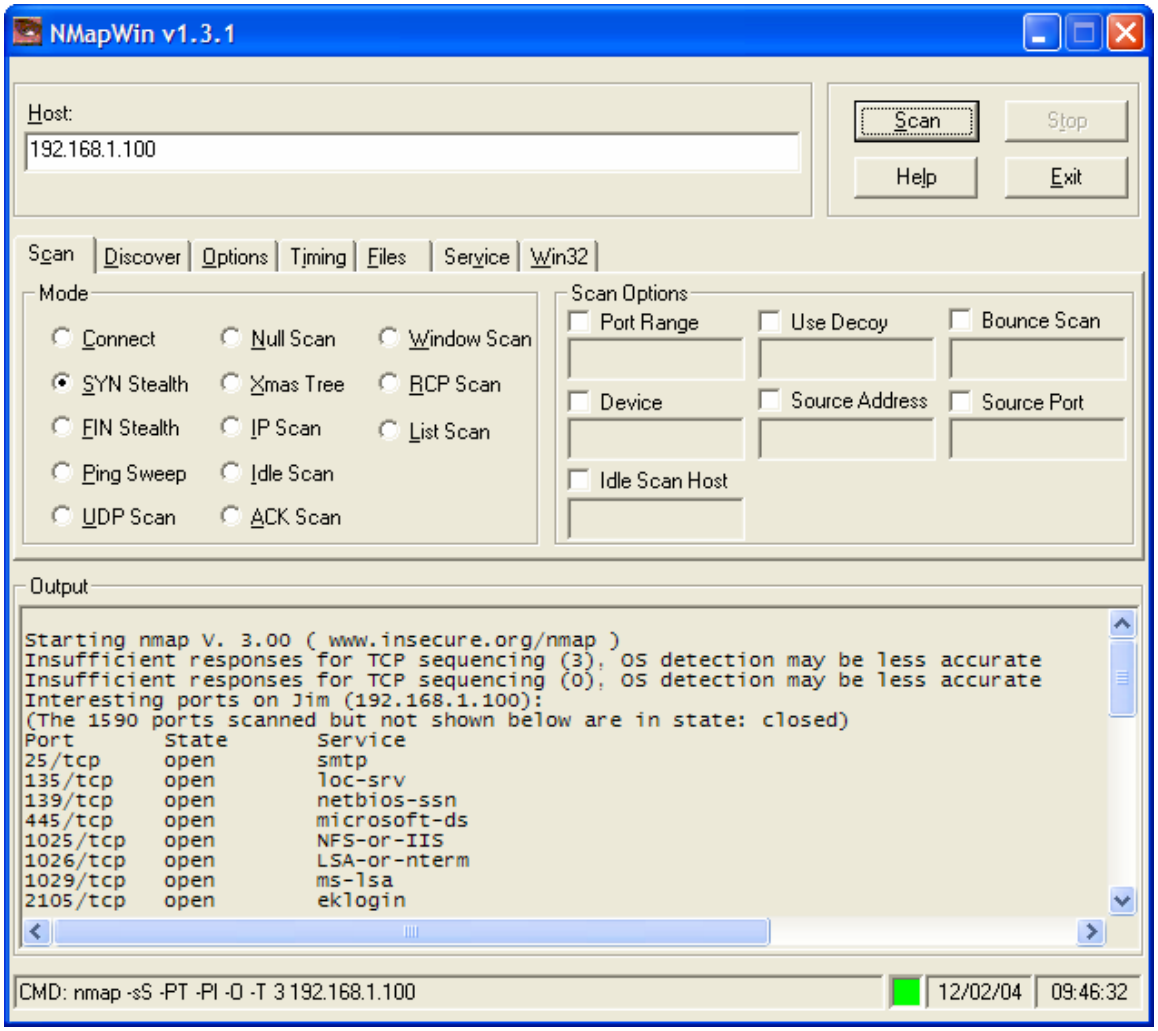

Figure 13. Nmap Scan Results

Figure 13 shows a sample scan of a single computer. Nmap can also be used to scan a range of IP addresses. This tool is very adaptable, allowing stealth pings and various types of scan techniques. SuperScan is another useful network-mapping tool and can be found at http://www.foundstone.com.

Another required tool is a password cracker. L0phtCrack (pronounced, "loft crack") from @Stake is a very good tool for this purpose. The tool can be downloaded

but a license is required. An equally effective freeware product is “john the ripper.” The home page for this product is http://www.openwall.com/john. The opening statement on that page describes the product thusly:

> John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. Besides several crypt(3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP LM hashes, plus several more with contributed patches.

Perhaps the next most useful tool is Netcat. Netcat can be found at http://netcat.sourceforge.net. It is described there as:

> Netcat is a featured networking utility which reads and writes data across network connections, using the TCP/IP protocol. It is designed to be a reliable "back-end" tool that can be used directly or easily driven by other programs and scripts. At the same time, it is a feature-rich network debugging and exploration tool, since it can create almost any kind of connection you would need and has several interesting built-in capabilities.

One of the “interesting” capabilities Netcat has is the ability to send data across the net to a host and port specified. Once a machine is penetrated, among the first tasks the hacker does is put Netcat on the victim machine. It can be named anything, of course. A wily hacker might call it Excell.exe or Win32Filter.exe. This naming obscurity will probably fool most users who would not be looking for programs of this type. If the program were stored in an alternate data stream [MAN01], it would be completely invisible to the user/owner of the victim box.

A very comprehensive list of tools can be found at http://www.hackingexposed.com/tools/tools.html. This list has been compiled by Stuart McClure and others at Foundstone, Inc.

In addition to the tools of penetration and compromise, the attackers may want to employ malware of some sort. “Back Orifice” is an easy tool to locate, install and use. “Rootkits” like “Adore” or “knark” and the many variations thereof, are readily available for use when attacking Linux or Unix systems. RootKits typically use the LKM

(Loadable Kernel Module) capability of Unix to load and install additional functionality in a running kernel. RootKits allow the attacker to add, change or delete utility programs. They often have stealth capability to hide their presence. Frequently, RootKits modify benign utilities like *chmod* or *ps* inserting functionality desired by the attacker.

There are thousands of other attack tools, so the attack plan should research the most useful and effective (and removable) for the exercise. For ideas, exercise participants should refer to the NIST ICAT (the acronym no longer has specific definition) database for a complete description of all known exploits, viruses, Trojans, worms and so on.

In addition to the aforementioned tools, a suite of tools from http://www.sysinternals.com is useful, well written and easily installed. Of this group, the Psexec tool is especially useful. The description provided by the vendor says, "The Pstools suite includes command-line utilities for listing the processes running on local or remote computers, running processes remotely, rebooting computers, dumping event logs, and more." Psexec allows the attacker to execute programs on the victim machine with the permission of the current user. Another tool from this suite is Pspasswd. Pspasswd lets the attacker change an account password on a local or remote system. The attacker can create batch files to run Pspasswd on computers they have penetrated and perform a mass change of the administrator or user passwords.

2. RCEL Activities for Scenario III

1. Define the needs and scope of the network [IRV03, HIL01, LAN01, BIS01, MAY01, 42, MCC01, MAN01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

2. Develop and write the attack plan [MCC01, MAN01]

   {L.O.s: 3G, 4G, 6G, 8N-11N, 14-18N, 21-24S, 21-28A, 32-37L}

3. Collect attack tools and exploits based on the attack plan [MCC01]

   {L.O.s: 4G, 19S, 20S, 22S, 23S, 24S, 26A, 37L}

4. Connect the hardware (without connecting the VPN to the internet or the router) [NAT12, LEI01]

   {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}

5. Configure the router and switch as needed [CIS01, LAR01, LON01]

   {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

6. Configure and test the workstations including minimal security and including tools specified in the attack plan [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]

   {L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

7. Configure the VPN according to the security plan and the requirements of the local network administrator [CIS01, KEN01, LAR01]

   {L.O.s: 1G, 4G, 5G, 7N, 9N, 10N, 11N, 14-18N, 23S, 24S, 27A, 28A, 29-34L}

8. Test the VPN with the victim organization without the RCEL router connected [KEN01, LAR01]

   {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L}

9. Connect the RCEL router when the exercise is ready to begin

   {L.O.s: 2G, 6G, 9N, 10N, 13N, 15-18N, 23S, 24S, 29L, 31L, 32L, 36L}

10. Test the security of the VPN [KEN01]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L, 37L}

11. Conduct the scheduled exercise [SAN01, IRV01, HIL01, BIS01, MAY01, NAT18, COM02, PFL01, NAT15, NAT16, NAT12, NAT03, NAT06, NAT10, LIT01, RUS01, MCC01, FRA01, NAT17, MAN01, LON01, ROS01, KEL01]

    {L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

12. Collect data during the exercise [MAN01]

    {L.O.s: 3G, 4G, 5G, 9-12N, 14N, 15-18N, 19-24S, 29L, 32L, 35L}

13. Disconnect the router and VPN when the exercise is concluded [CIS01, KEN01, LAR01]

    {L.O.s: 8N, 12N, 13N, 17N, 18N, 19S, 23S, 25A, 27A, 33L, 34L, 36L}

14. Analyze the success/failure of the attack plan [MCC01, MAN01]

    {L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

15. Analyze all attack results [MAN01]

    {L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L }

Note, if the attack strategy includes any self-replicating malware, great caution must be taken to prevent infection and spread among Scenario III host machines and inadvertent infection of other systems in the RCEL or elsewhere. This type of activity highlights the importance of the VPN and air-gapped lab configuration to protect other resources. That having been said, this lab configuration and exercise scenario is ideal for testing and evaluating the behavior of newly observed exploits and malware.

The learning objectives achieved in this scenario lean more to the attack side. There are still a lot of activities in setting up networks and VPNs but the sophistication of the security plan and contingency/continuity planning are eliminated.

D. SCENARIO IV – JOINT TEACHING EXERCISE

1. The Design

In this exercise, two academic/training organizations agree on a set of activities conducted between respective RCELs. This scenario relies on the flexibility of the

RCEL. There is no specific network configuration of the RCEL for this scenario, rather there are general guidelines that can be followed to create a successful inter-organization exercise.

A negotiated exercise is designed to address a particular need at a particular time. The participants design the RCEL to meet a mutually identified and specific training requirement. An example is training a group of programmers to manage a network remotely. Another example is providing lab functionality remotely to a small or poorly equipped organization for security training.

Referring to Figure 4 and Figure 5, it is possible to interpolate implementations of the RCEL for the specific exercises being planned. Most implementations will use VLANS to isolate network activity. The ACLs written for the router and switch are based on the amount of interaction agreed upon by the exercise participants.

In this scenario, a larger portion of effort will be in the analysis and design phases. There are many good resources to help with design of a secure network. One very useful and quick read is the NetScreen Whitepaper: Principles of Secure Network Design [NET01] available from http://www.netscreen.com. NetScreen is a security-focused manufacturer of network products and services. Three of their guiding principles are; “security is a process”, “effective security is Security-in-Depth” and “if you don’t know what you are protecting and why, you can’t protect anything.” The paper also covers seven steps to a more secure network design.

1. Audit – Determine what is important and why.

2. Partition – Separate the important from the unimportant.

3. Fix – Make your default-configured systems more secure.

4. Monitor – Add monitoring and logging systems to round out your security.

5. Protect – Make a plan, and a contact sheet for when attacks happen.

6. Check – Do a dry run – and attack your own network.

7. Update – Keep current, and re-evaluate your design as things change

With a document such as this, students have a good starting point for their work.

To provide added reliability, automatic failover of the routers may be desirable. If Cisco routers are used, as in the NPS RCEL, "hot standby routing protocol" (HSRP) is the proprietary Cisco protocol provided. In Scenarios IV, V and VI the network routers may be configured in an HSRP configuration, as seen in the Figure 14 [CIS05]. In this configuration, the network requires two routers and more set-up time. A virtual router is created and traffic is routed to that virtual machine. If Router A fails, there is no disruption of traffic as Router B automatically continues routing traffic.

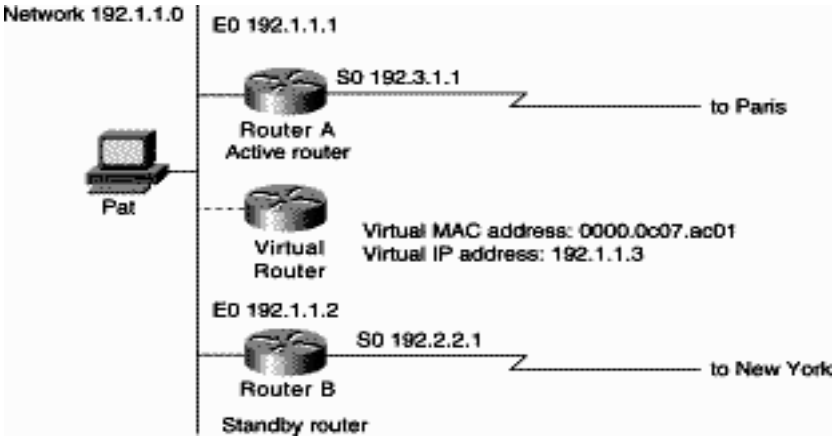

Figure 14. HSRP network configuration[CIS05], from http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm

2. RCEL Activities for Scenario IV

1. Determine the purpose of the exercise [SAN01, IRV01, HIL01, HIG01, BIS01, BIS03, MAY01, PFL01, NAT16, NAT13, NAT01, BLO02, CHI01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

2. Jointly define the scope and restrictions of the exercise

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

3. Generate MOU or MOA as required

   {L.O.s: 34-37L}

4. Define the needs and scope of the network [IRV03, HIL01, LAN01, BIS01, MAY01, 42, MCC01, MAN01, HOF01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

5. Design the network configuration [SAN01, HIL01, BIS01, MAY01, NAT16, NAT12, NAT04, NAT05, NAT08, MCC01, NAT17, ELE01, MOC01, POS01, LON01, GER01, LEI01, NET01]

   {L.O.s: ALL}

6. Write a security plan [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT12, NAT04, KEN01, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L }

7. Connect the hardware (without connecting the VPN to the internet or the router) [NAT12, ELE01]

   {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}

8. Configure router(s) as needed [SAN01, LEI02, COM02, CIS01, DEP01, DEF01, NAT06, NAT10, KEN01, LAR01, NAT17, MOC01, POS01, BER02, LON01, ROS01, NET01]

   {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

9. Configure the switch as needed including VLANs [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01]

   {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

10. Configure and test the workstations including security per the security plan [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05,

NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]

{L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

11. Implement and test the remainder of the security plan including incident response and operational continuity [SAN01, NAT18, COM02, DEP02, DEP01, NAT15, NAT16, NAT14, NAT03, NAT05, NAT06, RUS01, NAT17, NET01]

{L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16-18N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

12. Implement and test the data collection stations as needed [NAT15, MAN01]

{L.O.s: 1-6G, 7-11N, 13-18N, 20S, 22S, 25A, 26A, 30-32L, 35L, 37L}

13. Configure the VPN according to the security plan and the requirements of the local network administrator [DEF01, NAT10, KEN01, NAT17]

{L.O.s: 1G, 4G, 5G, 7N, 9N, 10N, 11N, 14-18N, 23S, 24S, 27A, 28A, 29-34L}

14. Test the VPN with the other exercise organization(s) without the RCEL router connected [KEN01]

{L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L}

15. Connect the RCEL router when the exercise is ready to begin

{L.O.s: 2G, 6G, 9N, 10N, 13N, 15-18N, 23S, 24S, 29L, 31L, 32L, 36L}

16. Test the security of the VPN [NAT10, KEN01, NAT17]

{L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L, 37L}

17. Conduct the scheduled exercise [IRV01, IRV03, HIL01, 13, 14, 15, 16, NAT13, BLO02, BLO01, SVI01, CHI01]

{L.O.s: ALL}

18. Collect data during the exercise [NAT15, MAN01]

{L.O.s: 3G, 4G, 5G, 9-12N, 14N, 15-18N, 19-24S, 29L, 32L, 35L}

19. Disconnect the router and VPN when the exercise is concluded[CIS01, KEN01, LAR01]

{L.O.s: 8N, 12N, 13N, 17N, 18N, 19S, 23S, 25A, 27A, 33L, 34L, 36L}

20. Analyze the success/failure of the security plan [NAT08, MAN01, DAY01]

{L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

21. Perform post-exercise forensics as needed [MAN01]

{L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L}

22. Debrief the exercise with both parties [SAN01, NAT16, NAT14, NAT12, NAT04, NAT05, NAT01]

{L.O.s: 4G, 6G, 8N, 10N, 12-15N, 19S, 20S, 24S, 25-27A, 29-31L, 33L, 36L, 37L}

23. Document at needed [DEP02]

{L.O.s: ALL}

E. SCENARIO V – EXTERNAL NETWORK VULNERABILITY ASSESSMENT

1. The Design

The RCEL may also be used by an organization as an active vulnerability assessment (VA) mechanism. For example, the XYZ organization has just implemented a new network and has requested an assessment to see if it can be readily penetrated before allowing it to go "live." XYZ configures a VPN connection to the RCEL and the network vulnerability assessment class (or assigned professionals), systematically attempt

penetration and enumeration of XYZ's network. The findings may be used for student assessment and helping XYZ determine their level of vulnerability.

Before the exercise is undertaken, a MOU/MOA should be negotiated and signed between the host RCEL and assessment target organizations. In this exercise, the local RCEL becomes, in effect, a contractor to the assessment target organization. Services provided depend on the specific need of the assessment target organization but must fall within the capability of the host RCEL and the administrative organization, e.g., NPS.

Services most likely to be requested and most easily supported include "red team" activities, training, or other specific remote assessment functions. In the discussion of this configuration a remote vulnerability assessment is assumed. NIST Special Publication 800-42 [NAT11] is an excellent guide for vulnerability assessment. The document provides a good list of VA activities and tools a host RCEL might use.

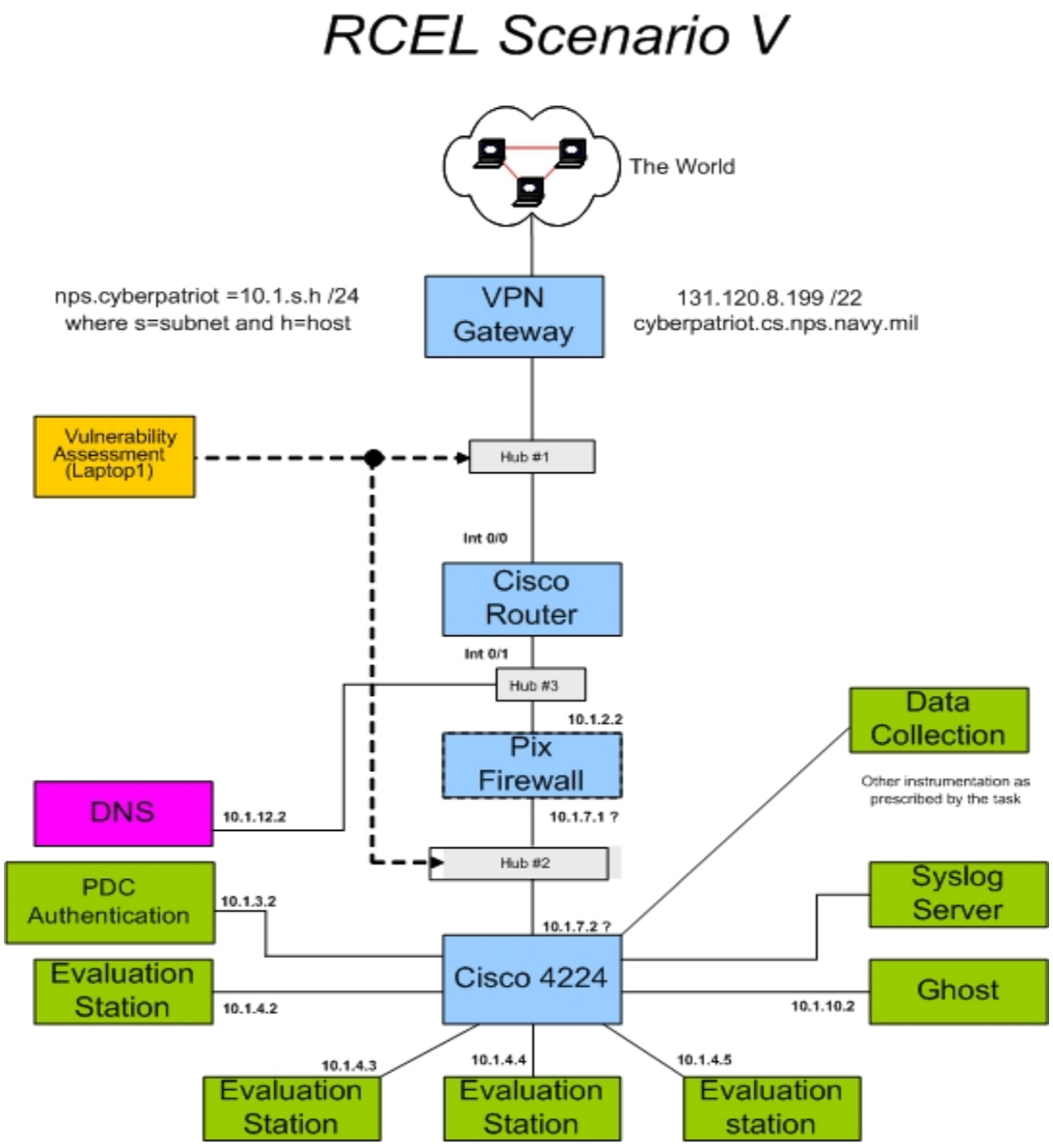

Figure 15. Scenario V - Vulnerability Assessment

Figure 15 shows a possible configuration for the VA Scenario. In this configuration, the security stations are restored and the workstations are dedicated to the task of evaluation. Note in Figure 15 the data collection station which represents any of a set of equipment (for example, a logic analyzer or sniffer) or applications (for example, forensic data collection applications, packet capture analysis and display, …) that might be used in the assessment process. In this scenario the RCEL network System

Administrator will want a standard compliment of network support functions implemented [DEP02], e.g., PDC, syslog, ghost, DNS, etc.

Probing and testing an external network is an intentionally intrusive procedure[NAT11] and may follow a pattern similar to that of Scenario III (attacking/hacking an external network). Major differences between Scenario III and Scenario V are intent (supportive versus malicious), probing with consent of the owners (activity step 3 below) of the network being evaluated, application of scientific method and the need for careful documentation including  spent, tester's name, vulnerabilities found, methodologies used, etc.

2. RCEL Activities for Scenario V

1. Determine the purpose of the exercise [SAN01, IRV01, HIL01, HIG01, BIS01, BIS03, MAY01, PFL01, NAT16, NAT13, NAT01, BLO02, CHI01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

2. Jointly define the scope and restrictions of the exercise [DEP03, DEP02, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

3. Generate MOU or MOA or other legal agreements as required

   {L.O.s: 34-37L}

4. Define the scope of the network and identify data collection requirements [IRV03, HIL01, LAN01, BIS01, MAY01, NAT15, 42, MCC01, MAN01, HOF01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

5. Define a management plan to document time and costs

   {L.O.s: 30-37L}

6. Begin documenting all management requested information, i.e., costs, time, contacts, signatures, etc

   {L.O.s: 27A, 35-37L}

7. Design the network configuration [SAN01, HIL01, BIS01, MAY01, NAT16, NAT12, NAT04, NAT05, NAT08, MCC01, NAT17, ELE01, MOC01, POS01, LON01, GER01, LEI01, NET01]

   {L.O.s: ALL}

8. Write a security plan for properly defending the host network [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT12, NAT04, KEN01, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

9. Get signed authorization to proceed from appropriate command/management levels [DEP02]

   {L.O.s: 27A, 35-37L}

10. Connect the hardware (without connecting the VPN to the internet or the router) [NAT12, ELE01]

    {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}

11. Configure router(s) and test as needed [SAN01, LEI02, COM02, CIS01, DEP01, DEF01, NAT06, NAT10, KEN01, LAR01, NAT17, MOC01, POS01, BER02, LON01, ROS01, NET01, CIS03]

    {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

12. Configure the switch as needed including VLANS [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01, CIS03]

{L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

13. Configure and test the workstations including security per the security plan [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]

    {L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

14. Configure and test all data collection devices [NAT15, MAN01]

    {L.O.s: 1-6G, 7-11N, 13-18N, 20S, 22S, 25A, 26A, 30-32L, 35L, 37L}

15. Implement and test the remainder of the security plan including incident response and operational continuity [SAN01, NAT18, COM02, DEP02, DEP01, NAT15, NAT16, NAT14, NAT03, NAT05, NAT06, RUS01, NAT17, NET01]

    {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16-18N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

16. Configure the VPN according to the security plan and the requirements of the local network administrator [DEF01, NAT10, KEN01, NAT17]

    {L.O.s: 1G, 4G, 5G, 7N, 9N, 10N, 11N, 14-18N, 23S, 24S, 27A, 28A, 29-34L}

17. Test the VPN with the requesting organization without the RCEL router connected [KEN01]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L}

18. Confirm the foreign network is isolated per the evaluation agreement (get a signature on this)

    {L.O.s: 35L, 36L}

19. Connect the RCEL router when the exercise is ready to begin

    {L.O.s: 2G, 6G, 9N, 10N, 13N, 15-18N, 23S, 24S, 29L, 31L, 32L, 36}

20. Test the security of the VPN [NAT10, KEN01, NAT17]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L, 37L}

21. Conduct the scheduled evaluation [DEP03, SAN01, COM01, MAR01, NAT18, COM02, DEP02, DEP01, NAT16, NAT14, NAT12, NAT03, NAT05, NAT08, NAT09, NAT10, LIT01, NAT17, DAY01, NET01, CIS03]

    {L.O.s: ALL}

22. Collect data during the exercise [NAT15, MCC01, MAN01]

    {L.O.s: 3G, 4G, 5G, 9-12N, 14N, 15-18N, 19-24S, 29L, 32L, 35L }

23. Disconnect the router and VPN when the exercise is concluded

    {L.O.s: 8N, 12N, 13N, 17N, 18N, 19S, 23S, 25A, 27A, 33L, 34L, 36L}

24. Document exercise activities and data collected

    {L.O.s: ALL}

25. Analyze the success/failure of the security plan [NAT08, MAN01, DAY01]

    {L.O.s: 6G, 7-18N, 19-24S, 25-28A, 29-37L}

26. Perform post-exercise forensics as needed [MCC01]

    {L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L}

27. Debrief the exercise with both parties [SAN01, NAT16, NAT14, NAT12, NAT04, NAT05, NAT01]

    {L.O.s: 4G, 6G, 8N, 10N, 12-15N, 19S, 20S, 24S, 25-27A, 29-31L, 33L, 36L, 37L}

28. Document as needed [DEP03, DEP02]

{L.O.s: ALL}

29. Prepare and send a professional report

{L.O.s: 27A}

30. Bill as indicated

{L.O.s: 27A}

F. SCENARIO VI – AGRESSIVE CYBER EXERCISE

1. The Design

This scenario is intended to be a very aggressive cyber exercise. Basically, the RCEL joins a VPN-based internet with other participating organizations and acts as both the aggressor and defender.

This type of exercise is very realistic. Any network deployed today with outside access will be attacked very quickly. Col. Hunt(USA) from JTF-CNO (Joint Task Force-Computer Network Operations) stated in an interview at NPS on March 9, 2004 that DoD networks are, on average, attacked within 23 minutes of going live. There are even cases of networks being compromised while being configured. Again, refer to Figure 4 and Figure 5, to give the student a realistic experience managing complex networks the NPS RCEL uses subnets and makes extensive use of VLANs. In Figure 16 [LAR01], we see a typical network configuration incorporating a perimeter router, a DMZ, a protected DMZ and a firewall.

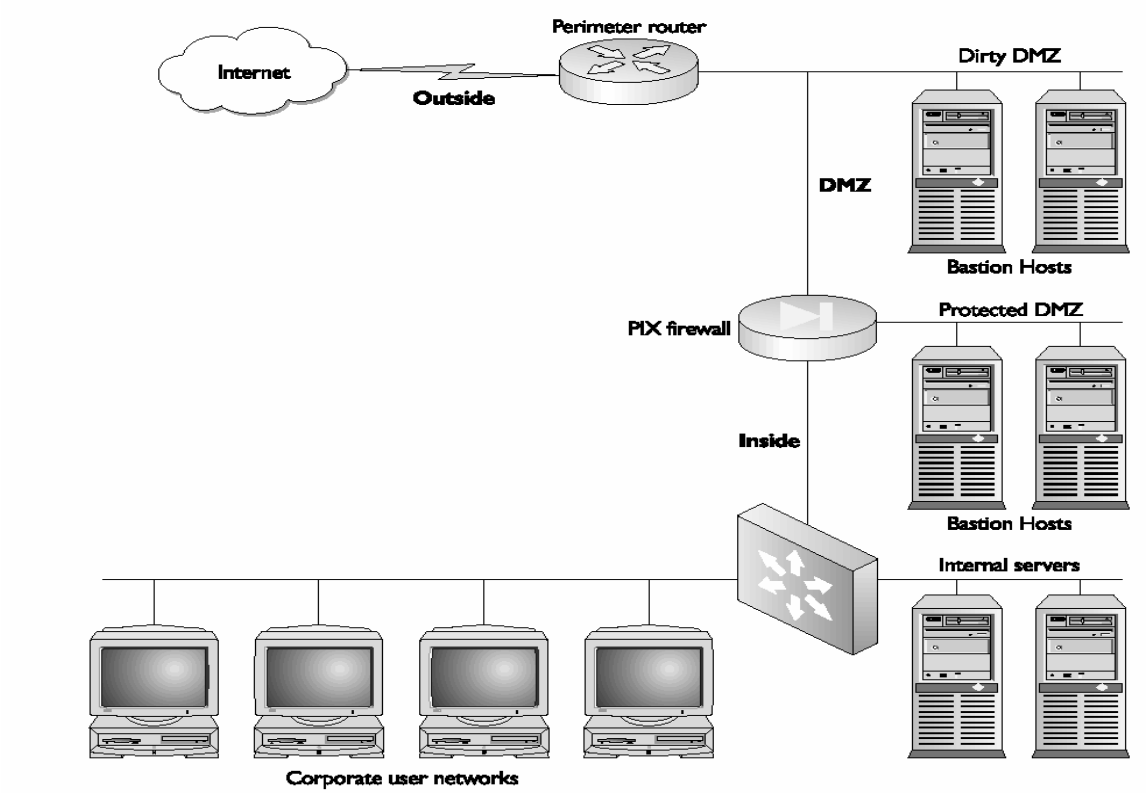

Figure 16. Typical Network Design with Perimeter Security[LAR01].

The organizations involved in this scenario will need to agree on terms and conditions of the exercise and a mutually agreed upon start and stop time. This scenario is very similar to the "capture the flag" type of exercise conducted annually at DEFCON (a hacker's conference, http://www.defcon.org/).

The network will likely need a full range of services: primary and backup domain controllers for windows-based authentication; DHCP server; mail server; syslog server; and DNS server. Supportive applications such as FTP, MySQL(or other database application), Web Services, and specific application servers may also be desired. This exercise provides a good testing ground for recently developed applications.

In the all out war exercise, the network can be configured with multiple redundancy/fail-over safeguards applied. These may include multiple HSRP routers, load-balanced routers and switches and similar advanced techniques. However, this redundancy adds a lot of complex network administration and few students will be up to the challenge without previous training. The increased complexity adds little to the

educational process. The only valid reason to add such extraordinary precautions would be if the students were experienced network administrators or if a particular network configuration was being tested or evaluated.

2. RCEL Activities for Scenario VI

1. Determine the purpose of the exercise [SAN01, IRV01, HIL01, HIG01, BIS01, BIS03, MAY01, PFL01, NAT16, NAT13, NAT01, BLO02, CHI01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

2. Jointly define the scope and restrictions of the exercise [DEP03, DEP02, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

3. Generate MOU or MOA or other legal agreements as required

   {L.O.s: 34-37L}

4. Define the scope of the network and identify data collection requirements [IRV03, HIL01, LAN01, BIS01, MAY01, NAT15, 42, MCC01, MAN01, HOF01]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

5. Design the network configuration [SAN01, HIL01, BIS01, MAY01, NAT16, NAT12, NAT04, NAT05, NAT08, MCC01, NAT17, ELE01, MOC01, POS01, LON01, GER01, LEI01, NET01, HOF01]

   {L.O.s: ALL}

6. Define network data vulnerability and risk [SAN01, NAT18, DEP02, NAT15, NAT12, NAT03, NAT05, NAT10, NAT17, HOF01]

   {L.O.s: }

7. Write a security plan for properly defending the host network emphasizing defense in depth [DEP03, SAN01, LEI02, NAT18, DEP01, NAT16, NAT12, NAT04, KEN01, NAT17]

   {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

8. Write attack plans as needed [MCC01, MAN01]

   {L.O.s: 3G, 4G, 6G, 8N-11N, 14-18N, 21-24S, 21-28A, 32-37L}

9. Get signed authorization to proceed from appropriate command/management levels [HOF01]

   {L.O.s: 35L, 37L}

10. Connect the hardware (without connecting the VPN to the internet or the router) [NAT12, ELE01]

    {L.O.s: 1G, 2G, 4G, 5G, 7N, 10N, 13N, 18N, 23S, 27A, 29L, 30L, 34L}

11. Configure router(s) and test as needed [SAN01, LEI02, COM02, CIS01, DEP01, DEF01, NAT06, NAT10, KEN01, LAR01, NAT17, MOC01, POS01, BER02, LON01, ROS01, NET01, CIS03]

    {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

12. Configure the switch as needed including VLANS [COM02, CIS01, DEF01, NAT04, NAT08, LAR01, NAT17, ROS01, CIS03]

    {L.O.s: 2G, 4G, 5G, 7N, 8-11N, 13-15N, 17N, 18N, 23S, 27A, 29-37L}

13. Configure and test the workstations including security per the security plan [SAN01, COM02, DEP01, NAT16, NAT14, NAT03, NAT05, NAT09, LIT01, RUS01, FRA01, POS01, BER02, LON01, ROS01, DAY01, KEL01, GER01]

{L.O.s: 1-6G, 7N, 8N, 10N, 13N, 14N, 15N, 17N, 18N, 20-24S, 25A, 27A, 29-37L}

14. Configure and test all data collection systems [NAT15, MAN01]

    {L.O.s: 1-6G, 7-11N, 13-18N, 20S, 22S, 25A, 26A, 30-32L, 35L, 37L}

15. Implement and test the remainder of the security plan including incident response and operational continuity [SAN01, NAT18, COM02, DEP02, DEP01, NAT15, NAT16, NAT14, NAT03, NAT05, NAT06, RUS01, NAT17, NET01]

    {L.O.s: 1G, 2G, 4-6G, 7N, 8N, 10N, 11N, 14N, 16-18N, 21-24S, 28A, 32L, 34L, 35L, 36L, 37L}

16. Configure the VPN according to the security plan and the requirements of the local network administrator [DEF01, NAT10, KEN01, NAT17]

    {L.O.s: 1G, 4G, 5G, 7N, 9N, 10N, 11N, 14-18N, 23S, 24S, 27A, 28A, 29-34L}

17. Test the VPN with the requesting organization without the RCEL router connected [KEN01, LAR01, NAT17]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L}

18. Confirm the foreign network is isolated per the exercise agreement (important, get a signature on this!) [HOF01]

    {L.O.s: 35L, 37L}

19. Connect the RCEL router when the exercise is ready to begin[]

    {L.O.s: 2G, 6G, 9N, 10N, 13N, 15-18N, 23S, 24S, 29L, 31L, 32L, 36}

20. Test the security of the VPN[]

    {L.O.s: 2G, 4G, 6G,, 9N, 10N, 11N, 16N, 20S, 23S, 25A, 27A, 28A, 29L, 30L, 32L, 34L, 35L, 37L}

21. Conduct the scheduled exercise[]

    {L.O.s: ALL}

22. Collect data during the exercise[]

    {L.O.s: 3G, 4G, 5G, 9-12N, 14N, 15-18N, 19-24S, 29L, 32L, 35L}

23. Disconnect the router and VPN when the exercise is concluded[]

    {L.O.s: 8N, 12N, 13N, 17N, 18N, 19S, 23S, 25A, 27A, 33L, 34L, 36L}

24. Document exercise activities and data collected[]

    {L.O.s: ALL}

25. Analyze the success/failure of the security plan [MCC01, MAN01]

    {L.O.s: 34-37L}

26. Perform post-exercise forensics as needed [MCC01, MAN01]

    {L.O.s: 8N, 9N, 12N, 14N, 19S, 20S, 23S, 24S, 34L, 36L, 37L}

27. Debrief the exercise with both parties

    {L.O.s: 35L, 37L}

28. Document at needed

    {L.O.s: 35L}

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

This thesis provides a useful laboratory support model for information assurance education programs. The reader may adopt or adapt any of the learning objectives, exercise scenarios or network topologies for use elsewhere.

Readers engaged in teaching information assurance may use the learning objectives, exercise scenarios and network topologies to reduce their developmental workload and enhance the teaching of information assurance.

Chapter II opens by demonstrating the need for more IA education. The connection between laboratory activities and learning theories is illustrated. Building on the strength of both Dale's and Bloom's research in learning and retention, the RCEL provides a venue to support traditional IA courses or to conduct targeted training.

To provide a useful model for learning objectives, a survey of critical information assurance topic areas is presented and then correlated to the information assurance curriculum of the Naval Postgraduate School. NPS provides a model from which to draw courses as the NPS information assurance curriculum is quite comprehensive. Learning objectives that support the possible activities within the RCEL are developed next. This model categorizes these learning objectives into five areas representing the type of learning processes and student activities taking place: computer laboratory skills, networks, security, analysis and leadership. In the process of categorizing the learning objectives, the emergence of the leadership category was especially interesting. When students work collectively or in groups in challenging, time sensitive settings, opportunities abound to strengthen their collective skill sets as officers and leaders.

To demonstrate the utility and flexibility of the RCEL concept, the paper presents six cyber-exercise scenarios. The premise of each scenario is that interaction with an external entity provides a high degree of reality and spontaneous experience during the exercise. The second important concept discussed is that using VPN technology, the interaction between an RCEL and an external facility (hopefully another RCEL) can be safe even when very powerful hacking tools are used.

Scenario I models a simple interaction between local users. Scenario II established a network with a defensive perimeter and demonstrates defensive techniques. Scenario III reverses the roles and shows an attack posture. Scenario IV allows two teaching organizations to define exercise activities that satisfy specific needs. Scenario V uses the RCEL to perform vulnerability testing. Scenario VI allows each participating RCEL to attack and defend its network.

To strengthen the RCEL model, each scenario's potential learning objectives are shown and cross referenced to NPS information assurance classes. This effort may prove useful to emerging information assurance education and training facilities.

Exercise scenarios provide, in a compressed timeframe, an opportunity to participate in every lifecycle phase of network security: analysis, design, construction, and operation. It is rare that an individual has the opportunity to see a network evolve from idea to operation. This experience can be enlightening, and the RCEL facility provides a safe and controlled environment where success is immediately recognized and failure is not catastrophic.

While a standard computer lab provides some educational benefits, a RCEL has the potential to provide a great deal more experiential learning. The main difference between a RCEL and a static computer lab is twofold: the RCEL is designed to be rapidly (even frequently) reconfigured and the opponent in any exercise is dynamic and real.

This paper has demonstrated that an effective RCEL facility can be deployed with minimal equipment and expenditure. Advanced RCEL configurations (Scenarios II – VI) are also demonstrated providing a range of possibilities to meet every information assurance laboratory need.

APPENDIX – ACRONYM DEFINITIONS

AAA - authentication, authorization, and accounting

ACM – Association for Computing Machines

ASP – Active Server Pages

ASP - Application Service Provider

BDC – Backup Domain Controller

CS – Computer Science

RCEL –Reconfigurable Cyber-Exercise Laboratory

CISR – Center fro INFOSEC Studies and Research

DITSCAP - DoD Information Technology Security Certification and Accreditation Process

DNS – Domain Name Service

DHCP – Dynamic Host Configuration Protocol

FTP – File Transfer Protocol

HSRP – Hot Standby Routing Protocol

HIDS – Host-based Intrusion Detection System

IA – Information Assurance

IDS – Intrusion Detection System

IKE – Internet Key Exchange

IEEE – Institute of Electrical and Electronic Engineers

IPSec – Internet Protocol Security, refer to RFC 2401

IOS – Internetwork Operating System (®Cisco Systems)

JTF-CNO – Joint Task Force – Computer Network Operations

LAN – Local Area Network

LO – Learning Objective

MOA – Memorandum of Agreement

MOU – Memorandum of Understanding

MOVES – Modeling, Virtual Environments and Simulation

NIDS – Network Intrusion Detection System

NIPRNet - Non-Secure Internet Protocol Router Network

NIST – National Institute of Standards and Technology

NSTISSI - National Security Telecommunications and Information Systems Security Instruction

NPS – Naval Postgraduate School

PDC – Primary Domain Controller

PSTN - Public Switched Telephone Network

RIPv2 – Routing Information Protocol Version II

SIPRNet - Secret Internet Protocol Router Network

SSAA - System Security Authorization Agreement

SSH – Secure Shell

SSL – Secure Socket Layer

TLD – Top level Domain

VoIP - Voice over Internet Protocol

VLAN – Virtual Local Area Network

VPN - Virtual Private Network

WAP – Wireless Access Point

LIST OF REFERENCES

[ARB01] Arbaugh W. Narendar Shankar, Y.C. Justin Wan *Your 802.11 Wireless Network has No Clothes.* Department of Computer Science University of Maryland. March 30, 2001

[BER01] Berkowitz, Bruce. *The DI and "IT:" Failing to Keep Up With the Information Revolution.* http://www.cia.gov/csi/studies/vol47no1/article07.html. Retrieved January 24, 2004

[BER02] Berners-Lee, T. Fielding, R. and Frystyk, H. *Hypertext Transfer Protocol HTTP/1.0*, RFC-1945. USC Information Sciences Institute. May 1996.

[BIS01] Bishop, M. and Heberlein, L. T., *An Isolated Network for Research*, *19th National Information Systems Security Conference*, Baltimore, MD, October 22-25, 1996, pp. 349-360.

[BIS02] Bishop, Matt. *Computer security in introductory programming classes*. In Workshop on Education in Computer Security, pages 1–2, Monterey, CA, USA, January 1997.

[BIS03] Bishop, Matt. *Teaching Computer Security,* Proceedings of the Ninth IFIP International Symposium on Computer Security, IFIP/Sec '93 , pp. 43-52 (May 1993).

[BLO01] Bloom, Bengamin S. Mesia, Bertram B. and Krathwohl, David R. (1964). *Taxonomy of Educational Objectives* (two vols: The Affective Domain & The Cognitive Domain). New York. David McKay.

[BLO02] Bloom, B.S. (Ed.) (1956) *Taxonomy of educational objectives: The classification of educational goals: Handbook I, cognitive domain*. New York ; Toronto: Longmans, Green.

[CIS01] Cisco Online Documentation (CDROM).

[CIS02] Cisco Systems Inc., *Introduction to the Cisco Network-Based IPSec VPN Solution Release 1.5*. http://www.cisco.com/univercd/cc/td/doc/product/vpn Accessed January 14, 2004.

[CIS03] Cisco Whitepaper. *SAFE:Extending the Security Blueprint to Small,Midsize, and Remote-User Networks*. 2001 Cisco Systems, Inc.

[CIS04] Cisco Online Documentation, *Cisco Router Password Recovery* http://www.cisco.com/warp/public/474/. Last accessed December 2003.

[CIS05] http://www.cisco.com/univercd/cc/td/doc/cisintwk/ics/cs009.htm. *Using HSRP for Fault-Tolerant IP Routing.* Last accessed March 2004.

[CNS01] CNSS Instruction No. 4009 *National Information Assurance Glossary*, CNSS Secretariat (I42). National Security Organization. Revised May 2003

[COM01] Common Criteria, http://www.commoncriteria.org/ December 2003.

[COM02] Computer Security Resource Center http://csrc.nist.gov/. January 24 2004.

[COM03] Computing Curricula 2001, *Final Report December 1, 2001*. The Joint Task Force on Computing Curricula IEEE Computer Society Association for Computing Machinery. Retrieved February 1, 2004 from http://www.computer.org/education/cc2001/final/index.htm.

[DAL01] Dale, E. (1969). *Audio-Visual Methods in Teaching (3rd Edn.)*. Holt, Rinehart, and Winston.

[DAY01] Dayton, Doug. *Information Technology Audit Handbook*. ISBN-0-13-614314-8. Prentice Hall, Englewood Cliffs. 1997.

[DEF01] Defense Information Systems Organization. DoDI 8550.bb, *Ports, Protocols, and Services Management. Draft*, March 20, 2003.

DEN01. Denning, Peter J. *Great Principals of Computing*, Communications of the ACM Vol. 46 No. 11. http://cne.gmu.edu/pjd/PUBS/CACMcols/cacmNov03.pdf. Retrieved March 10 2003.

[DEP01] Department Of Defense. Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, March 21, 1988.

[DEP02] Department of Defense. Directive 5200.40, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) November 30 1997.

[DEP03] Department Of Defense. Directive 8500.1 Information Assurance. October 24, 2002.

[DJB01] Burnstein, D. *http://www.djbdns.org/*. Last accessed March 2004

[DRO01] Droms, R. *Dynamic Host Configuration Protocol*, RFC 2131 March 1997.

[DU01] Du, Wenlaing. *Using An Instructional Operating System In Teaching Computer Security Courses.* Systems Assurance Institute Department of Electrical Engineering and Computer Science Syracuse University.

[ELE01] Electronics Industries Association as requested by the Computer Communications Industry Association in 1985. *EIA/TIA 568 Commercial Building Telecommunications Wiring Standard. Retrieved* February 3, 2004 from http://www.webopedia.com/TERM/C/Cat_5.html .

[FED01] Federal Bureau of Investigation, Computer Security Institute. *2003 CSI/FBI Computer Crime and Security Survey*. Retrieved January 25, 2004 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf .

[FRA01] Fraser, B. *Site Security Handbook.* SEI/CMU RFC-1296. September, 1997

[GER01] Gerhards, R., *The syslog Protocol draft-ietf-syslog-protocol-02.txt*., February 2004.

[HIG01] Higgins, J., *Information Security as a Topic in Undergraduate Education of Computer Scientists*, Twelfth National computer Security Conference, Baltimore, MD, October 10, 1989, pp. 553-557.

[HIL01] Hill J. M. D., Carver, Jr. C. A., Humphries J. W., and Pooch U. W. *Using an isolated network laboratory to teach advanced networks and security*. In Proceedings of the 32nd SIGCSE Technical Symposium on Computer Science Education, pages 36–40, Charlotte, NC, USA, February 2001.

[HOF01] Hoffer, J., Goerge, J., Valacicho, J. (1996)*Modern System Analysis and Design*. Menlo Park, The Benjamin/Cummings Publishing Company Inc.

[IPA01] IPAdventures Whitepaper. *ISAKMP/Oakley*. Copyright 1997-2001 by Ken Camp.

[IRV01] Irvine, C.E. *Amplifying Security Education in the Laboratory*, Proceeding of the IFIP TCll WC 11.8 First World Conference on Information Security Education, Kista, Sweden, June 1999, pp 139-146.

[IRV02] Irvine, C., The *Reference Monitor Concept as a Unifying Principle in* Computer Security. ftp://taurus.cs.nps.navy.mil/pub/irvine/99/wise99_RMCUnifySecEd.pdf.

[IRV03] Irvine C. E., Stemp R., Warren D. F. *Teaching Introductory Computer Security at a Department of Defense University*, Naval Postgraduate School Monterey, CA, Naval Postgraduate School-CS-97-002, April 1997

[IRV04] Irvine, C., Levin, T., *Toward a Taxonomy and Costing Method for Security Services*., Naval Postgraduate School and Anteon Corp., Proceedings of the Computer Security Applications Conference, Phoenix, AZ, December 1999.

[IRV05] Irvine C.E., Chin, S. K.Frinke D.A. *An Information Security Education Initiative for Engineering and Computer Science* Naval Postgraduate School Technical Report, the Naval Postgraduate SchoolCS-97-003, Naval Postgraduate School, Monterey, CA, December 1997.

[KEL01] Kelsey, J., Callas, J., The *syslog Protocol and Signed syslog Messages draft-ietf-syslog-sign-13.txt*. NIST and PGP Corp., October 2003

[KEN01] Kent, S. and Atkinson, R.. RFC 2401: *Security Architecture for the Internet Protocol*. Corporation for National Research Initiatives, Reston, Virginia, USA, November 1998.

[LAN01] Landwehr C. E., Bull A. R., McDermott J. P., and Choi W. S. *A taxonomy of computer program security flaws.* ACM Computing Surveys, 26(3):211–254, September 1994.

[LAR01] Larson, Robert E. Cockcroft, L. (2003). *All in One Cisco Certified Security Professional Certification Exam Guide*. New York: Osborne/McGraw Hill.

[LEI01] Leiner, B., *Policy Issues in Interconnecting Networks*. RIACS. RFC-1124. September 1989.

[LEI02] Leiwo J. and Zheng Y. *A framework for the management of information security*. In Information Security -- Proceedings of the First International Workshop, number 1396 in Lecture Notes in Computer Science, pages 232--245. Springer--Verlag, 1997.

[LIT01] LittleW0lf (a.k.a. Dennis W. Mattison), *Network Printers and Other Peripherals -Vulnerability and Fixes* ltlw0lf@cox.net published 8 July 2002

[LON01] Lonvick, C. *The BSD syslog Protocol*, RFC-3164. Cisco Systems, August 2001

[MCC01] McClure, Stuart. Scambray, Joel. Kurtz, George. (2003). *Hacking Exposed, Network Security Secrets & Solutions. 4th Edition*. New York:Osborne/McGraw-Hill.

[MAN01] Mandia, K., Prosise, C. Pepe, M. *Incident Response and Computer Forensics 2nd Edition*. Osborne/McGraw Hill. 2003, ISBN 0-07-222696-X.

[MAR01] Marsh, R. T., *Critical Foundations: Protecting America's Infrastructure*, President's Commission on Critical Infrastructure Protection, October 1997.

[MAY01] Mayo J. and Kearns P. *A secure unrestricted advanced systems laboratory*. In Proceedings of the 30th SIGCSE Technical Symposium on Computer Science Education, pages 165–169, New Orleans, USA,March 24-28 1999.

[MIC01] Microsoft Corporation, *Security Management for ASPs*, retrieved February 14, 2004 from http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/ecommerce/maintain/operate/aspsec.asp .

[MOC01] Mockapetris, P., *Domain Names - Concepts and Facilities*, STD 13/RFC 1034, USC/Information Sciences Institute, November 1987.

[NAT01] National Institute of Standards and Technology Special Publication 800-16. *Information Technology Security Training Requirements.* Retrieved January 25, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT02] National Institute of Standards and Technology Special Publication 800-25. *Federal Organization Use of Public Key Technology for Digital Signatures and Authentication.* Retrieved November 1, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT03] National Institute of Standards and Technology Special Publication 800-26. *Security Self-Assessment Guide for Information Technology Systems.* Retrieved October 10, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT04] National Institute of Standards and Technology Special Publication 800-27. *Engineering Principles for Information Technology Security (A Baseline for Achieving Security).* Retrieved October 1, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT05] National Institute of Standards and Technology Special Publication 800-30. *Risk Management Guide for Information Technology Systems.* Retrieved October 11, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT06] National Institute of Standards and Technology Special Publication 800-31. *Intrusion Detection Systems (IDS).* Retrieved October 1, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT07] National Institute of Standards and Technology Special Publication 800-32. *Introduction to Public Key Technology and the Federal PKI Infrastructure.* Retrieved October 1, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT08] National Institute of Standards and Technology Special Publication 800-33. *Underlying Technical Models for Information Technology Security.* Retrieved October 7, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT09] National Institute of Standards and Technology Special Publication 800-35. *Guide to Information Technology Security Services.* Retrieved October 12, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT10] National Institute of Standards and Technology Special Publication 800-41. *Guidelines on Firewalls and Firewall Policy.* Retrieved October 11, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT11] National Institute of Standards and Technology Special Publication 800-42. *Guideline on Network Security Testing.* Retrieved March 13, 2004 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT12] National Institute of Standards and Technology Special Publication 800-47. *Security Guide for Interconnecting Information Technology Systems.* Retrieved November 1, *2003* from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT13] National Institute of Standards *and* Technology Special Publication 800-50. *Building an Information Technology Security Awareness and Training Program.* Retrieved November 12, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT14] National Institute of Standards and Technology Special Publication 800-55. *Security Metrics Guide for Information Technology Systems.* Retrieved November 12, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT15] National Institute of Standards and Technology Special Publication 800-61. *Computer Security Incident Handling Guide.* Retrieved January 23, 2004 from http://csrc.nist.gov/publications/drafts/draft_sp800-61.pdf .

[NAT16] National Institute of Standards and Technology Special Publication 800-64. *Security Considerations in the Information System Development Life Cycle.* Retrieved November 12, 2003 from http://csrc.nist.gov/publications/nistpubs/index.html .

[NAT17] National Security Agency SNAC. *60 Minute Security Guide*. Updated July 12, 2002 Version 1.2.

[NAT18] National Security Agency. *Security Recommendation Guides* http://www.nsa.gov/snac/index.html January 2004.

[NAT19] National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, *National Information Systems Security Glossary*, September 2002.

[NET01] NetScreen Whitepaper *Principles of Secure Network Design*, August 27th, 2001, CASE-260-002. Retrieved November 5, 2003 from http://www.netscreen.com .

[OLD01] Older, S., Shiu-Kai Chin. *Outcomes-based Assessment as an Assurance Education Tool*. World Conference on Information Security Education 2003

[PFL01] Pfleeger, Charles P., Pfleeger Shari L. (2003) *Security in Computing 3rd ed*. Upper Saddle River: Prentice Hall.

[POS01] Postel, J. and J. Reynolds. *File Transfer Protocol(FTP)*, IETF, RFC 959 (superceding RFC 765), Oct. 1985.

[PRE01] President's information technology advisory committee, report to the president *Information Technology Research:Investing in Our Future*. February 1999.

[ROS01] Rose, M., New, D. *Reliable Delivery for syslog*. RFC-3195. Dover Beach Consulting, Inc. November 2001.

[RUS01] RU*Secure*™ - *Information Security Officer's Manual (ISO Manual).* Retrieved January 3, 2004 from http://www.RUsecure.com .

[SAN01] SANS Institute. *Information Security Management Checklist* :BS 7799.2:2002 for SANS. Retrieved March 1 2004 from http://www.sans.org/score/checklists/ISO_17799_checklist.pdf .

[SAL01] Saltzer, J.H. and M.D. Schroeder, *The protection of information in computer systems*, Proceedings of the IEEE 63 (9) (1975) 1278--1308.

[SFS01] http://www.ehr.nsf.gov/ehr/due/programs/sfs. Last accessed January 2004.

[SVI01] Svinicki, Marilla D., (ed. 1990). *The Changing Face of College Teaching. New Directions for Teaching and Learning No. 42*. San Francisco, CA: Jossey-Bass.

[VPN01] VPN Consortium, *VPN Technologies: Definitions and Requirements*. Retrieved January 2004 from http://www.vpnc.org/vpn-technologies.html .

[WEI01] Weimer, M. 1990. *Improving College Teaching.* San Francisco,CA, Jossey-Bass.

[YNG01] Yngström Björck, Yngstrm Louise, and Bjrck Fredrik. *The Value* and *Assessment of Information Security Education.* Department of Computer and Systems Sciences, Stockholm University Royal Institute of Technology, Electrum 230, SE-164 40 Kista, Sweden.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvior, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Dr. Cynthia Irvine
   Naval Postgraduate School
   Monterey, CA

4. J. D. Fulp, Instructor
   Naval Postgraduate School
   Monterey, CA

5. Col. Karen Burke
   Naval Postgraduate School
   Monterey, CA

6. Ann Rideout
   SPAWAR SCC
   Charleston, SC

8. Dr. Ernest McDuffie
   National Science Foundation
   Arlington, VA

9. John Mildner
   SPAWAR
   Charleston, SC